Lecciones populares de matemáticas

RESOLUCIÓN DE ECUACIONES EN NÚMEROS ENTEROS

A. O. Guelfond

$$\left[x_0^2\right]^2 + \left[y_0^2\right]^2 = z_0^2$$

Editorial MIR Moscú

Lecciones populares de matemáticas

RESOLUCIÓN DE ECUACIONES EN NÚMEROS ENTEROS

A. O. Guelfond

Editorial MIR Moscú

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ
ВЫПУСК 8

А. О. ГЕЛЬФОНД

РЕШЕНИЕ УРАВНЕНИЙ В ЦЕЛЫХ ЧИСЛАХ

ИЗДАТЕЛЬСТВО «НАУКА»
МОСКВА

LECCIONES POPULARES DE MATEMÁTICAS
Volumen 8

A. O. GUELFOND

RESOLUCIÓN DE ECUACIONES EN NÚMEROS ENTEROS

Traducido del ruso por el ingeniero
Cristóbal García Galán
Primera edición electrónica septiembre de 2018

Primera edición 1979
Segunda edición 1984

EDITORIAL MIR
MOSCÚ

Impreso en la URSS
На испанском языке

Índice general

Introducción 5

1 Ecuaciones con una incógnita 9

2 Ecuaciones de primer grado con dos incógnitas 11

3 Ejemplos de ecuaciones de segundo grado con tres incógnitas 23

4 Ecuaciones del tipo $x^2 - Ay^2 = 1$ 29

5 Caso general para ecuaciones de segundo grado 43

6 Ecuaciones con dos incógnitas 55

7 Ecuaciones algebraicas de grado superior al segundo 61

Introducción

La teoría de los números examina principalmente las propiedades aritméticas de los números de la serie natural, es decir, de los números enteros positivos, y pertenece a una de las ramas más antiguas de las Matemáticas. Uno de los problemas centrales de la llamada teoría analítica de los números es el problema de la distribución de números primos en la serie natural. Se llama número primo cualquier número entero positivo mayor que uno, que se divide sin resto solamente por sí mismo y por la unidad. El problema de la distribución de números primos en serie natural consiste en determinar si es justo o no el comportamiento del conjunto de números primos menores que cierto número N, cuando N tiene valores grandes. El primer resultado en esta dirección lo hallamos ya en los trabajos de Euclides (siglo IV a. d. n. e.), concretamente la demostración de que la serie de números primos es infinita; el segundo resultado, después de Euclides, fue obtenido por el gran matemático ruso P. L Chebishev en la segunda mitad del siglo XIX. Otro de los problemas fundamentales de la teoría de los números es la expresión de números enteros como suma de números enteros de un determinado tipo, por ejemplo, la expresión de números impares como suma de tres números primos. Este último problema, llamado de Goldbach, fue resuelto por uno de los más ilustres representantes de la teoría de los números, el matemático soviético I. M. Vinográdov.

El libro que ofrecemos al lector está también dedicado a una de las partes más interesantes de la teoría de los números, concretamente a la resolución de ecuaciones en números enteros.

Uno de los problemas más difíciles de la teoría de los números es la resolución, en números enteros, de ecuaciones algebraicas con coeficientes enteros y con más de una incógnita. Al estudio de estos problemas se dedicaron intensamente los más eminentes matemáticos de la antigüedad, por ejemplo, el matemático griego Pitágoras (siglo VI a.d.n.e.), Diofanto de Alejandría (siglo II–III d.n.e.) y los mejores matemáticos

de épocas más cercanas a la nuestra, entre ellos P. Fermat (siglo XVII), L. Euler (siglo XVIII), I. L. Lagrange (siglo XVIII) y otros. No obstante al esfuerzo de muchas generaciones de eminentes matemáticos, en esta rama de las Matemáticas no existen métodos comunes semejantes al método de sumas trigonométricas — propuesto por I. M. Vinogradov — que permite resolver los más variados problemas de la teoría analítica de los números.

El problema relacionado con la solución de ecuaciones en números enteros está completamente resuelto solamente para ecuaciones de segundo grado con dos incógnitas. Para ecuaciones de cualquier grado con una incógnita, este problema no representa interés esencial alguno, ya que puede ser resuelto mediante una cantidad finita de pruebas. Para ecuaciones de grado superior al segundo con dos o más incógnitas, es sumamente difícil no solamente el problema de hallar todas las soluciones en números enteros, sino también problemas más simples como es la determinación de la existencia de un conjunto finito o infinito de dichas soluciones.

La solución de ecuaciones en números enteros tiene no solamente interés teórico. Pues ecuaciones de este tipo a veces se dan en la física.

El interés teórico que presentan las ecuaciones de números enteros es lo suficiente alto puesto que estas ecuaciones están estrechamente ligadas a muchos problemas de la teoría de los números. Además, las partes elementales de la teoría de estas ecuaciones, expuestas en este libro, pueden ser utilizadas con éxito para ampliar los conocimientos en matemáticas de los alumnos de escuelas medias y estudiantes de institutos pedagógicos.

El libro contiene la descripción de algunos resultados fundamentales, obtenidos en la teoría de la resolución de ecuaciones en números enteros. Los teoremas formulados en él, van acompañados por sus respectivas demostraciones en aquellos casos, cuando estas demostraciones son lo suficiente simples.

CAPÍTULO 1

Ecuaciones con una incógnita

Examinemos la ecuación de primer grado con una incógnita

$$a_1x + a_0 = 0. \qquad (1.1)$$

Sean sus coeficientes a_1 y a_0 números enteros. Entonces la solución de esta ecuación

$$x = -\frac{a_0}{a_1}$$

será un número entero sólo cuando a_0 es divisible sin resto por a_1. Es decir, la ecuación (1.1) no siempre puede ser resuelta en números enteros, por ejemplo, de dos ecuaciones $3x - 27 = 0$ y $5x + 21 = 0$, la primera tiene solución entera $x = 9$, mientras que la segunda carece de tales soluciones.

Esta misma circunstancia se presenta también en ecuaciones de un grado superior al primero, pues si la ecuación cuadrada $x^2 + x - 2 = 0$ tiene soluciones enteras $x_1 = 1$, $x_2 = -2$, la ecuación $x^2 - 4x + 2 = 0$ no posee tales soluciones, ya que sus raíces $x_{1,2} = 2 \pm \sqrt{2}$ son irracionales.

El problema de hallar raíces enteras en ecuaciones de n-ésimo grado con coeficientes enteros,

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \quad (n \geqslant 1) \qquad (1.2)$$

se resuelve con facilidad. En efecto, sea $x = a$ una raíz entera de esta ecuación. En-

tonces

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$
$$a_0 = -a(a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_1 x)$$

Por La última igualdad vemos que a_0 se divide por a sin resto, por lo tanto, cada raíz entera de la ecuación (1.2) es divisor del término independiente de dicha ecuación. Para hallar las soluciones enteras de esta ecuación es preciso elegir aquellos divisores a_0, con los cuales, realizando sustituciones en la ecuación, ésta se transforma en identidad. Así, por ejemplo, entre todos los divisores del término independiente de la ecuación

$$x^1 0 + x^7 + 2x^3 + 2 = 0,$$

que son 1, −1, 2 y −2, solamente −1 es raíz. Por consiguiente, esta ecuación tiene la única raíz entera $x = -1$. Utilizando este mismo método es fácil demostrar que la ecuación

$$x^6 - x^5 + 3x^4 + x^2 - x + 3 = 0$$

no tiene solución en números enteros.

Considerablemente mayor interés lo representa la resolución, en números enteros, de ecuaciones con muchas incógnitas.

CAPÍTULO 2

Ecuaciones de primer grado con dos incógnitas

Examinemos la ecuación de primer grado con dos incógnitas

$$ax + by + c = 0 \tag{2.1}$$

en la que a y b son números enteros diferentes de cero y c, un número entero arbitrario. Vamos a considerar que los coeficientes a y b no tienen más divisores comunes que la unidad[1]. En efecto, siendo el máximo común divisor de estos coeficientes $d = (a, b)$ diferente de la unidad, las igualdades $a = a_1 d$ y $b = b_1 d$ son verídicas, la ecuación (2.1) adquiere la forma como sigue

$$(a_1 x + b_1 y)d + c = 0$$

y puede tener soluciones enteras sólo cuando c es divisible por d. Así, pues, cuando $(a, b) = d \neq 1$ todos los coeficientes de la ecuación (2.1) deben dividirse por d sin resto y simplificando la ecuación (2.1) por d obtendremos la ecuación

$$a_1 x + b_1 y + c_1 = 0 \quad \left(c_1 = \frac{c}{d}\right),$$

cuyos coeficientes a_1 y b_1 son números primos entre sí.

Veamos primeramente el caso cuando $c = 0$. La ecuación (2.1) toma la forma:

$$ax + by = 0. \tag{2.2}$$

[1]Los números a y b con esta particularidad se llaman números *primos entre sí*; considerando (a, b) como máximo común divisor de a y b, para los números primos entre sí, tendremos que $(a, b) = 1$.

Resolviendo esta ecuación respecto a x obtenemos

$$x = -\frac{b}{a}y.$$

Queda claro que x tendrá valores enteros si, y sólo si, y se divide por a sin resto. Pero cualquier número entero y, múltiplo de a, puede ser expresado de la siguiente forma

$$y = at,$$

en la que t adquiere valores enteros arbitrarios ($t = 0, \pm 1, \pm 2, \ldots$). Poniendo este valor de y en la ecuación anterior, o sea,

$$x = -\frac{b}{a}at = -bt,$$

obtenemos las fórmulas que contienen todas las soluciones enteras de la ecuación (2.2):

$$x = -bt, \quad y = at \quad (t = 0, \pm 1, \pm 2, \ldots).$$

Pasemos ahora al caso cuando $c \neq 0$.

Demostraremos primeramente que para hallar todas las soluciones enteras de la ecuación (2.1) es suficiente hallar una solución cualquiera de esta ecuación, o sea, hallar unos números enteros x_0, y_0, tales que

$$ax_0 + by_0 + c = 0.$$

2.0.1 Teorema: Sean a y b números primos entre sí y $[x_0, y_0]$ cualquier solución[2] de la ecuación 2.1

$$ax + by + c = 0.$$

Entonces, las fórmulas

$$x = x_0 - bt, \quad y = y_0 + at, \tag{2.3}$$

siendo $t = 0, \pm 1, \pm 2, \ldots$, dan todas las soluciones de la ecuación (2.1).

Demostración: Sea $[x, y]$ solución arbitraria de la ecuación (2.1). Entonces de las igualdades

$$ax + by + c = 0 \quad \text{y} \quad ax_0 + by_0 + c = 0$$

[2]El par de números enteros x e y que satisface una ecuación se llama *solución* y se designa por $[x, y]$.

tenemos que

$$ax - ax_0 + by - by_0 = 0; \quad y - y_0 = \frac{a(x_0 - x)}{b}.$$

Como $y - y_0$ es un número entero y a y b números primos entre sí, la expresión $x_0 - x$ debe dividirse por b sin resto, es decir, $x_0 - x$ adquiere la forma

$$x_0 - x = bt,$$

en la que t es número entero. Pero entonces

$$y - y_0 = \frac{abt}{b} = at,$$

y, por consiguiente, tenernos

$$x = x_0 - bt \quad \text{e} \quad y = y_0 + at.$$

Así queda demostrado que cualquier solución $[x, y]$ tiene la misma forma que las fórmulas (2.3). Falta demostrar por último, que cualquier par de números $[x_1, y_1]$, obtenido a base de las fórmulas (2.3), siendo $t = t_1$ número entero, es solución de la ecuación (2.1). Para comprobarlo pongamos los valores $x_1 = x_0 - bt_1$ e $y_1 = y_0 + at_1$ en el primer miembro de la ecuación (2.1):

$$ax_1 + by_1 + c = ax_0abt_1 + by_0 + abt_1 + c = ax_0 + by_0 + c,$$

entonces, como $[x_0, y_0]$ es solución, tenemos que $ax_0 + by_0 + c = 0$ y por lo tanto

$$ax_1 + by_1 + c = 0,$$

es decir, $[x_1, y_1]$ es solución de la ecuación (2.1), con lo cual el teorema queda completamente demostrado. □

En resumen, siendo conocida una solución de la ecuación $ax + by + c = 0$, las demás pueden hallarse empleando progresiones aritméticas, cuyos términos comunes tienen la siguiente expresión

$$x = x_0 - bt \quad \text{e} \quad y = y_0 + at \quad (t = 0, \pm 1, \pm 2, \ldots).$$

Observemos que en caso de ser $c = 0$, las fórmulas de las soluciones halladas anteriormente

$$x = -bt \quad \text{e} \quad y = at$$

pueden ser obtenidas a partir de las que acabamos de recibir, o sea,

$$x = x_0 - bt \quad \text{e} \quad y = y_0 + at,$$

si se toman $x_0 = y_0 = 0$; cosa posible puesto que los valores $x = 0$ e $y = 0$ son, sin duda, solución de la ecuación

$$ax + by = 0.$$

Veamos, a continuación, cómo hallar una solución $[x_0, y_0]$ cualquiera de la ecuación (2.1) en el caso general cuando $c \neq 0$.

Para ello comenzaremos por un ejemplo.

Sea dada la ecuación

$$127x - 52y + 1 = 0.$$

Transformemos la relación entre los coeficientes de las incógnitas.

Primeramente separamos la parte entera de la fracción impropia $\frac{127}{52}$:

$$\frac{127}{52} = 2 + \frac{23}{52}$$

Luego cambiamos la fracción propia $\frac{23}{52}$ por otra igual a ella $\frac{1}{\frac{52}{23}}$. Obtenemos entonces

$$\frac{127}{52} = 2 + \frac{1}{\frac{52}{23}}.$$

Hagamos las mismas transformación es con la fracción impropia obtenida en el denominador $\frac{52}{23}$:

$$\frac{52}{23} = 2 + \frac{6}{23} = 2 + \frac{1}{\frac{23}{6}}$$

Ahora la fracción inicial tendrá la forma

$$\frac{127}{52} = 2 + \frac{1}{2 + \frac{1}{\frac{23}{6}}}$$

Realicemos los mismos razonamientos para ıa fracción $\frac{23}{6}$:

$$\frac{23}{6} = 3 + \frac{5}{6} = 3 + \frac{1}{\frac{6}{5}}.$$

Tenemos entonces

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\frac{6}{5}}}}$$

Separando la parte entera de la fracción impropia $\frac{6}{5}$,

$$\frac{6}{5} = 1 + \frac{1}{5},$$

obtenemos como resultado final

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

La expresión obtenida se llama fracción *continua finita* o *fracción continua*. Suprimiendo el último término de esta fracción, o sea un quinto, transformamos la fracción continua que acabamos de recibir en una fracción ordinaria y la restamos de la fracción inicial $\frac{127}{52}$:

$$2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1}}} = 2 + \cfrac{1}{2 + \cfrac{1}{4}} = 2 + \frac{4}{9} = \frac{22}{9},$$

$$\frac{127}{52} - \frac{22}{9} = \frac{1143 - 1144}{52 \cdot 9} = -\frac{1}{52 \cdot 9}.$$

Reduciendo, a continuación, la expresión obtenida a un denominador común y suprimiendo este denominador, obtenemos:

$$127 \cdot 9 - 52 \cdot 22 + 1 = 0.$$

Comparando la igualdad obtenida con la ecuación

$$127x - 52y + 1 = 0,$$

vemos que $x = 9$ e $y = 22$ son solución de esta ecuación y, de acuerdo con el teorema, todas sus soluciones estarán incluidas en las progresiones:

$$x = 9 + 52t, \quad y = 22 + 127t \quad (t = 0, \pm 1, \pm 2, \ldots).$$

El resultado obtenido permite deducir que, en el caso general, para hallar la solución de la ecuación $ax + by + c = 0$ es preciso desarrollar en fracción continua la relación entre los coeficientes de las incógnitas, suspender su último término y hacer los mismos cálculos que fueron hechos anteriormente.

Para demostrar esta suposición nos serán precisas algunas de las propiedades de las fracciones continuas.

Examinemos la fracción irreducible $\frac{a}{b}$. Designando por q_1 el cociente y por r_2 el resto de la división de a por b tendremos:

$$a = q_1 b + r_2, \quad r_2 < b.$$

Supongamos, a continuación, que q_2 es el cociente y r_3 el resto de la división de b por r_2. Entonces

$$b = q_2 r_2 + r_3, \quad r_3 < r_2;$$

exactamente lo mismo

$$\begin{array}{rcl} r_2 & = & q_3 r_3 + r_4, \quad r_4 < r_3, \\ r_3 & = & q_4 r_4 + r_5, \quad r_5 < r_4, \\ \multicolumn{3}{c}{\dots\dots\dots\dots\dots\dots\dots\dots} \end{array}$$

Las magnitudes q_1, q_2, ... se llaman *cocientes incompletos*. El procedimiento de formación de estos cocientes, dado anteriormente, se llama *algoritmo de Euclides*. Los restos de las divisiones r_2, r_3, ... cumplen las desigualdades

$$b > r_2 > r_3 > r_4 > \cdots \geqslant 0, \tag{2.4}$$

es decir, forman una serie decreciente de números no negativos.

Como la cantidad de números enteros no negativos y no superiores a b no puede ser infinita. en un determinado momento, la formación de cocientes incompletos se suspende puesto que se anula el siguiente resto r. Sea r_n el último resto distinto de cero en la serie (2.4); entonces $r_{n+1} = 0$ y el algoritmo de Euclides para los números a y b adquiere la forma

$$\left.\begin{array}{rcl} a & = & q_1 b + r_2, \\ b & = & q_2 r_2 + r_3, \\ r_2 & = & q_3 r_3 + r_4, \\ \multicolumn{3}{c}{\dots\dots\dots\dots\dots\dots\dots} \\ r_{n-2} & = & q_{n-1} r_{n-1} + r_n, \\ r_{n-1} & = & q_n r_n. \end{array}\right\} \tag{2.5}$$

Pasando las igualdades obtenidas a la forma

$$
\begin{aligned}
\frac{a}{b} &= q_1 + \frac{1}{\frac{b}{r_2}}, \\
\frac{b}{r_2} &= q_2 + \frac{1}{\frac{r_2}{r_3}}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}, \\
\frac{r_{n-1}}{r_n} &= q_n
\end{aligned}
$$

y sustituyendo en la primera de estas igualdades el valor de $\frac{b}{r_2}$ por su valor correspondiente, dado por ta segunda; en ésta el valor de $\frac{r_2}{r_3}$ por su valor correspondiente, dado por la tercera, y así sucesivamente, obtendremos el desarrollo de $\frac{a}{b}$ en una fracción continua:

$$
\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}
$$

La expresión obtenida después de suprimir en una fracción continua todos sus términos a partir de uno se llama *fracción reducida*. En nuestro caso, la primera fracción reducida δ_1 se obtiene limitando la fracción dada a partir de $\frac{1}{q_2}$:

$$
\delta_1 = q_1 < \frac{a}{b}.
$$

La segunda a partir de $\frac{1}{q_3}$:

$$
\delta_2 = q_1 + \frac{1}{q_2} > \frac{a}{b}.
$$

Lo mismo

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q3}} < \frac{a}{b},$$

$$\delta_4 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}} > \frac{a}{b}$$

y así sucesivamente.

El procedimiento de formación de fracciones reducidas trae consigo la aparición de desigualdades explícitas:

$$\delta_1 < \delta_3 < \cdots < \delta_{2k-1} < \frac{a}{b};$$

$$\delta_2 > \delta_4 > \cdots > \delta_{2k} > \frac{a}{b}.$$

Expresemos la k-ésima fracción reducida δ_k de la siguiente forma

$$\delta_k = \frac{P_k}{Q_k} \quad (1 \leqslant k \leqslant n),$$

y hallemos la ley de formación de numeradores y denominadores en las fracciones reducidas. Para ello transformamos las primeras fracciones reducidas $\delta_1, \delta_2, \delta_3$:

$$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}; \quad P_1 = q_1; \quad Q_1 = 1;$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1q_2 + 1}{q_2} = \frac{P_1}{Q_2}; \quad P_2 = q_1q_2 + 1; \quad Q_2 = q_2;$$

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = q_1 + \frac{q_3}{q_2q_3 + 1} = \frac{q_1q_2q_3 + q_1 + q_3}{q_2q_3 + 1} = \frac{P_3}{Q_3};$$

$$P_3 = q_1q_2q_3 + q_1 + q_3; \quad Q_3 = q_2q_3 + 1,$$

de donde obtenemos:

$$P_3 = P_2q_3 + P_1; \quad Q_3 = Q_2q_3 + Q_1.$$

Utilizando el método de inducción matemática[3] demostraremos que las relaciones de este mismo tipo

$$P_k = P_{k-1}q_k + P_{k-2}, \quad Q_k = Q_{k-1}q_k + Q_{k-2} \tag{2.6}$$

[3]Véase el libro de esta misma serie de I. S. Sominski «Método de inducción matemática», Editorial Mir, 1975.

son válidas para todos $k \geqslant 3$.

En efecto, supongamos que las igualdades (2.6) se cumplen a un cualquier $k \geqslant 3$. De la definición de las fracciones reducidas se desprende directamente, que sustituyendo en la expresión las magnitudes q_k por $q_k + \dfrac{1}{q_{k+1}}$ esta expresión se convierte en δ_{k+1}. Conforme a la suposición por inducción, tenemos que

$$\delta_k = \frac{P_k}{Q_k} = \frac{P_{k-1}q_k + P_{k-2}}{Q_{k-1}q_k + Q_{k-2}}$$

Sustituyendo aquí q_k por $q_k + \dfrac{1}{q_{k+1}}$, resulta:

$$\delta_{k+1} = \frac{P_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + P_{k-2}}{Q_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + Q_{k-2}} = \frac{P_k + \dfrac{1}{q_{k+1}}P_{k-1}}{Q_k + \dfrac{1}{q_{k+1}}Q_{k-1}} = \frac{P_k q_{k+q1} + P_{k-1}}{Q_k q_{k+q1} + Q_{k-1}}.$$

De aquí siendo $\delta_{k+1} = \dfrac{P_{k+1}}{Q_{k+1}}$ resulta que

$$P_{k+1} = P_k q_k + P_{k-1}, \quad Q_{k+1} = Q_k q_{k+1} + Q_{k-1}.$$

Así, pues, de la validez de las igualdades (2.6), para cualquier $k \geqslant 3$, se deduce su validez para $k + 1$. Pero siendo $k = 3$ las igualdades (2.6) son válidas, y, por consiguiente, lo serán también en todos los casos cuando $k \geqslant 3$.

A continuación demostraremos que la diferencia entre dos fracciones reducidas consecutivas $\delta_k - \delta_{k-1}$ cumple la proporción

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \ (k > 1). \tag{2.7}$$

En efecto,

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}}$$

Valiéndonos de las fórmulas (2.6), transformemos el numerador de la fracción obtenida:

$$P_k Q_{k-1} - Q_k P_{k-1} = (P_{k-1}q_k + P_{k-2})Q_{k-1} - (Q_{k-1}q_k + Q_{k-2})P_{k-1} = \\ = -(P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}).$$

La expresión comprendida entre paréntesis se obtiene sustituyendo k por $k-1$ en la fórmula inicial. Repitiendo las mismas transformaciones en las expresiones obtenidas, tendremos evidentemente, una sucesión de igualdades:

$$\begin{aligned} P_k Q_k - Q_k P_{k-1} =& (-1)(P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}) = \\ =& (-1)^2(P_{k-2}Q_{k-3} - Q_{k-2}P_{k-3}) = \dots \\ \dots =& (-1)^{k-2}(P_2 Q_1 - Q_2 P_1) = \\ =& (-1)^{k-2}(q_1 q_2 + 1 - q_2 q_1) = (-1)^{k-2}. \end{aligned}$$

De esto se deduce que

$$\delta_k - \delta_{k-1} = -\frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}} = \frac{(-1)^{k-2}}{Q_k Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}$$

Cuando el desarrollo de $\frac{a}{b}$ en fracción continua posee n términos, la n-ésima fracción reducida δ_n coincide con $\frac{a}{b}$. Utilizando la igualdad (2.7), siendo $k = n$, tenemos:

$$\begin{aligned} \delta_n - \delta_{n-1} =& \frac{(-1)^n}{Q_n Q_{n-1}}. \\ \frac{a}{b} - \delta_{n-1} =& \frac{(-1)^n}{b Q_{n-1}}. \end{aligned} \tag{2.8}$$

Volvamos ahora a la resolución de la ecuación

$$ax + by + c = 0, \ (a, b) = 1. \tag{2.9}$$

Expresemos la proporción (2.8) como sigue

$$\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{b Q_{n-1}}.$$

Reduciendo esta proporción a un denominador común y omitiéndolo, nos resulta

$$aQ_{n-1} - bP_{n-1} = (-1)^n, \quad aQ_{n-1} + b(-P_{n-1}) + (-1)^{n-1} = 0.$$

Multiplicando la relación obtenida por $(-1)^{n-1}c$, tenemos:

$$a[(-1)^{n-1}cQ_{n-1}] + b[(-1)^n cP_{n-1}] + c = 0.$$

De aquí se deduce que el *par de números* $[x_0, y_0]$, siendo

$$x_0 = (-1)^{n-1}cQ_{n-1} - bt, \quad y_0 = (-1)^n cP_{n-1}, \tag{2.10}$$

es una solución de la ecuación (2.9) y, conforme al teorema, todas las soluciones de esta ecuación tienen la forma siguiente

$$x = (-1)^{n-1} c Q_{n-1} - bt, \quad y = (-1)^n c P_{n-1} + at \quad (t = 0, \pm 1, \pm 2, \ldots).$$

El resultado obtenido resuelve completamente el problema de hallar todas las soluciones en números enteros, de ecuaciones de primer grado con dos incógnitas. Pasemos ahora a examinar algunas ecuaciones de segundo grado.

CAPÍTULO 3

Ejemplos de ecuaciones de segundo grado con tres incógnitas

EJEMPLO 1. Examinemos la ecuación de segundo grado con tres incógnitas:

$$x^2 + y^2 = z^2. \tag{3.1}$$

Geométricamente, la solución en números enteros de esta ecuación se puede interpretar como la determinación de todos los triángulos de Pitágoras, es decir, de triángulos rectangulares cuyos catetos x, y e hipotenusa z se expresan en números enteros.

Designando por d al máximo común divisor de x e y: $d = (x, y)$, entonces

$$x = x_1 d, \quad y = y_1 d,$$

y la ecuación (3.1) toma la forma:

$$x_1^2 d^2 + y_1^2 d^2 = z^2.$$

De aquí se deduce que z^2 es divisible por d^2 y, por lo tanto, z es múltiplo de d, es decir, $z = z_1 d$.

Ahora la ecuación (3.1) se puede expresar de la forma:

$$x_1^2 d^2 + y_1^2 d^2 = z_1^2 d^2;$$

simplificando por d^2, tenemos

$$x_1^2 + y_1^2 = z_1^2.$$

La ecuación obtenida tiene la misma forma que la inicial, además, las magnitudes x_1 e y_1 no tienen más divisores comunes que 1. Por lo tanto, para resolver la ecuación (3.1) es suficiente limitarse al caso cuando x e y son números primos entre sí. Supongamos que $(x, y) = 1$. Entonces, por lo menos, una de las magnitudes x o y (por ejemplo x) es impar. Pasando y^2 al segundo miembro de la ecuación (3.1), obtenemos:

$$x^2 = z^2 - y^2; \quad x^2 = (z+y)(z-y). \tag{3.2}$$

Designando por d_1 al máximo común divisor de $z + y$ y $z - y$, tenemos que

$$z + r = ad_1 \quad \text{y} \quad z - y = bd_1, \tag{3.3}$$

siendo a y b números primos entre sí.

Sustituyendo en la ecuación (3.2) $z + y$ y $z - y$, por sus valores resulta:

$$x^2 = abd_1^2.$$

Como a y b no tienen divisores comunes, la igualdad obtenida es válida sólo cuando a y b son cuadrados perfectos[1]:

$$a = u^2, \quad b = v^2$$

Pero entonces

$$x^2 = u^2v^2d_1^2$$

y

$$x = uvd_1. \tag{3.4}$$

Hallemos ahora los valores y y z de las igualdades (3.3). La suma de estas igualdades nos da:

$$2z = ad_1 + bd_1 = u^2d_1 + v^2d_1; \quad z = \frac{u^2 + v^2}{2}d_1. \tag{3.5}$$

Restando la segunda igualdad de la primera en las igualdades (3.3) obtenemos:

$$2y = ad_1 - bd_1 = u^2d_1 - v^2d_1; \quad y = \frac{u^2 - v^2}{2}d_1. \tag{3.6}$$

Puesto que en la ecuación (3.4) x es impar, resulta que u, v y d_1 también son impares. Además $d_1 = 1$, ya que de lo contrario de las ecuaciones

$$x = uvd_1 \quad \text{e} \quad y = \frac{u^2 - v^2}{2}d_1$$

[1] Es sabido que el producto de la multiplicación de dos números primos entre sí puede ser cuadrado perfecto solo si cada factor es cuadrado perfecto.

se deduciría que las magnitudes x e y tienen por divisor común $d_1 \neq 1$, lo que contradice la suposición de que son primas entre sí. Los números u y v están relacionados con los números primos entre sí a y b por las igualdades

$$a = u^2, \quad b = v^2$$

y, por consiguiente, son también primos entre sí; $v < u$, ya que $b < a$, lo cual se deduce de las igualdades (3.3).

Sustituyendo $d_1 = 1$ en las igualdades (3.4), (3.5) y (3.6) obtenemos las *fórmulas*:

$$x = uv, \quad y = \frac{u^2 + v^2}{2} \quad \text{y} \quad z = \frac{u^2 + v^2}{2}, \tag{3.7}$$

las cuales, *siendo u y v ($v < u$) números impares y primos entre sí, permiten obtener todos los números enteros positivos x, y, z, libres de divisores comunes, que verifican la ecuación (3.1)*. Realizando simple sustitución de x, y, z en la ecuación (3.1), es fácil comprobar que, siendo cualesquiera u y v, los números de las fórmulas (3.7) verifican esta ecuación.

Para valores iniciales de u y v las fórmulas (3.7) se reducen a las siguientes igualdades, frecuentemente utilizadas:

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \quad (v = 1,\ u = 3), \\ 5^2 + 12^2 &= 13^2 \quad (v = 1,\ u = 5), \\ 15^2 + 8^2 &= 17^2 \quad (v = 3,\ u = 5). \end{aligned}$$

Como ya indicamos anteriormente, las fórmulas (3.7) dan solamente aquellas soluciones de la ecuación

$$x^2 + y^2 = z^2,$$

en las que números x, y y z no tienen divisores comunes. Todas las demás soluciones de esta ecuación en números enteros y positivos se obtienen multiplicando las soluciones, contenidas en las fórmulas (3.7), por un factor común arbitrario d.

De la misma forma que obtuvimos todas las soluciones de la ecuación (3.1) pueden ser obtenidas todas las soluciones para otras ecuaciones del mismo tipo.

EJEMPLO 2. Hallemos todas las soluciones de la ecuación

$$x^2 + 2y^2 = z^2 \tag{3.8}$$

en números enteros positivos x, y, z primos entre sí dos a dos.

Observamos que si x, y, z son solución de la ecuación (3.8) y si no tienen divisor común diferente de 1, éstos son al mismo tiempo primos entre sí dos a dos. En efecto, si x e y son múltiplos de un número primo $p > 2$, de la igualdad

$$\left(\frac{x}{p}\right)^2 + 2\left(\frac{y}{p}\right)^2 = \left(\frac{z}{p}\right)^2$$

se desprende que z es múltiplo de p, puesto que el primer miembro de esta igualdad es número entero. Lo mismo sucederá si x y z o y y z son divisibles por p.

Observemos que x deberá ser número impar para que el máximo común divisor de x, y, z sea igual a 1. En efecto, si x es par el primer miembro de la ecuación (3.8) será número par y, por lo tanto, z también lo será. Pero entonces x^2 y z^2 son múltiplos de 4. De ello se deduce que $2y^2$ debe ser divisible por 4, o sea, que y también debe ser número par. Es decir, si x es par, entonces todos los números x, y, z deben también ser pares. En conclusión, en una solución sin divisor común diferente a 1,

x debe ser impar. De esto se deduce que z también debe ser impar. Pasando x^2 al segundo miembro de la ecuación (3.8), obtenemos:

$$2y^2 = z^2 - x^2 = (z + x)(z - x).$$

Ahora bien, el máximo común divisor de $z + x$ y $z - x$ es 2. En efecto, sea d su máximo común divisor. Entonces

$$z + x = kd, \quad z - x = ld,$$

aquí k y l son números enteros. Sumando y restando estas igualdades, tendremos que:

$$2z = d(k + l), \quad 2x = d(k - l).$$

Pero z y x son números impares primos entre sí. Por eso, el máximo común divisor de $2x$ y 2z es 2. Y, por lo tanto, $d = 2$.

Así pues, $\frac{z+x}{2}$ o $\frac{z-x}{2}$ es impar y, por consiguiente, o son primos entre sí los números

$$z + x \quad \text{y} \quad \frac{z - x}{2}$$

o lo son los números

$$\frac{z + x}{2} \quad \text{y} \quad z - x.$$

En el primer caso, de la igualdad

$$(z - x)\frac{z - x}{2} = y^2$$

se deduce que

$$z + x = n^2 \quad \text{y} \quad z - x = 2m^2,$$

y en el segundo, de la igualdad

$$\frac{z+x}{2}(z-x) = y^2$$

se deduce que

$$z + x = 2m^2 \quad \text{y} \quad z - x = n^2,$$

siendo n y m números enteros; m, impar y $n > 0$, $m > 0$. Resolviendo estos dos sistemas de ecuaciones con relación a x y z, y hallando y, tendremos que o bien

$$z = \frac{1}{2}(n^2 + 2m^2), \quad x = \frac{1}{2}(n^2 - 2m^2), \quad y = mn,$$

o bien

$$z = \frac{1}{2}(n^2 + 2m^2), \quad x = \frac{1}{2}(m^2 - 2n^2), \quad y = mn,$$

siendo m número impar. Uniendo estas dos formas que representan la solución x, y, z, obtenemos la fórmula general

$$x = \pm\frac{1}{2}(n^2 - 2m^2), \quad y = mn, \quad z = \frac{1}{2}(n^2 + 2m^2),$$

en la que m es impar. Pero para que z y x sean números enteros es preciso que n sea par. Suponiendo que $n = 2b$ y $m = a$, obtendremos definitivamente las *fórmulas generales que dan todas las soluciones x, y, z de la ecuación (3.8) en números enteros y positivos sin divisor común mayor que* 1:

$$x = \pm(a^2 - 2b^2), \quad y = 2ab, \quad z = a^2 + 2b^2, \tag{3.9}$$

aquí a y b son números positivos primos entre sí y a un número impar. Siendo éstas las condiciones, las magnitudes de a y b se eligen arbitrariamente, pero de tal modo que x sea positivo. Las fórmulas (3.9) dan, efectivamente, todas las soluciones x, y, z en números enteros positivos y primos entre sí puesto que por una parte, hemos demostrado que en este caso x, y, z deben expresarse por las fórmulas (3.9) y, por otra, si eligimos a y b de tal modo que satisfagan nuestras condiciones, entonces x, y, z serán, en efecto, primos entre sí y solución de la ecuación (3.8).

CAPÍTULO 4

Ecuaciones del tipo $x^2 - Ay^2 = 1$. Determinación de todas las soluciones de esta ecuación

Pasamos ahora a la resolución en números enteros de ecuaciones de segundo grado con dos incógnitas del tipo

$$x^2 - Ay^2 = 1, \tag{4.1}$$

donde A es un número entero positivo, no siendo cuadrado perfecto. Para determinar cómo resolver las ecuaciones deberemos primeramente examinar el método de desarrollo en fracción continua de números irracionales, tal como $\sqrt{A}$. Conforme al algoritmo de Euclides, cualquier número racional se desarrolla en fracción continua con un número finito de términos. Otra es la cuestión cuando se trata de números irracionales. Las fracciones continuas que les corresponden son infinitas. Desarrollemos, por ejemplo, en fracción continua el número irracional $\sqrt{2}$.

Transformando la identidad explicita

$$\left(\sqrt{2} - 1\right)\left(\sqrt{2} + 1\right) = 1,$$

$$\sqrt{2} - 1 = \frac{1}{\sqrt{2} + 1},$$

$$\sqrt{2} - 1 = \frac{1}{2 + \left(\sqrt{2} - 1\right)}$$

y sustituyendo la diferencia $\sqrt{2} - 1$, obtenida en el denominador, por otra expresión igual a ella como identidad, o sea,

$$\frac{1}{2 + \left(\sqrt{2} - 1\right)}$$

tendremos

$$\sqrt{2} - 1 = \cfrac{1}{2 + \cfrac{1}{2 + \left(\sqrt{2} - 1\right)}}; \qquad \sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \left(\sqrt{2} - 1\right)}}$$

Sustituyendo nuevamente la expresión entre paréntesis en el denominador de la última igualdad por una fracción de la misma identidad e igual a dicha expresión, tendremos:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \left(\sqrt{2} - 1\right)}}}$$

Continuando este procedimíento obtendremos el siguiente desarrollo de en fracción continua infinita:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}} \tag{4.2}$$

Observemos que el procedimiento de desarrollo en fracción continua, aplicado anteriormente, está basado en la utilización de identidades del tipo

$$\left(\sqrt{m^2 + 1} - m\right)\left(\sqrt{m^2 + 1} + m\right) = 1,$$

y es válido no para todas las irracionalidades $\sqrt{A}$. Dicho procedimiento puede ser utilizado en aquellos casos cuando el número entero A puede expresarse como $A = m^2 + 1$, siendo m un número entero diferente de cero. (En particular, $m = 1$ nos da el desarrollo e $\sqrt{2}$; $m = 2$, el desarrollo de $\sqrt{5}$ y así sucesivamente.) No obstante, para el caso general, existen también procedimientos relativamente no complicados para desarrollar $\sqrt{A}$ en fracción continua[1].

[1]Véase, por ejemplo, el libro de I. V. Arnold «Teoría de los números», cap. VI (Uchpedguiz, 1939), o el libro de A. Ya. Jinchin «Fracciones continuas» (Gostejizdat, M. 1949).

Lo mismo que en el caso de fracciones continuas finitas, formemos para la fracción continua infinita (4.2) una sucesión de fracciones reducidas $\delta_1, \delta_2, \delta_3$, ..., o sea:

$$\begin{aligned} &\delta_1 = 1, && \delta_1 < \sqrt{2};\\ &\delta_2 = 1 + \frac{1}{2} = \frac{3}{2}, && \delta_2 > \sqrt{2};\\ &\delta_3 = 1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5}, && \delta_3 < \sqrt{2};\\ &\delta_4 = \cdots = \frac{17}{12} && \delta_4 > \sqrt{2}; \end{aligned} \tag{4.3}$$

y así sucesivamente.

Conforme al procedimiento de formación de fracciones reducidas se deduce que

$$\delta_1 < \delta_3 < \cdots < \sqrt{2};$$
$$\delta_2 > \delta_4 > \cdots > \sqrt{2}.$$

En general, si tenemos dado el desarrollo en fracción continua infinita para cierto número irracional α,

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}$$

entonces para las fracciones reducidas son justas las desigualdades:

$$\begin{aligned} \delta_1 < \delta_3 < \cdots < \delta_{2k+1} < \cdots < \alpha < \cdots\\ \cdots < \delta_{2k} < \cdots < \delta_k < \delta_2. \end{aligned} \tag{4.4}$$

Expresemos la fracción reducida δ_k de la forma

$$\delta_k = \frac{P_k}{Q_k}.$$

Las relaciones (2.6)

$$P_k = P_{k-1}q_k + P_{k-2} \quad \text{y} \quad Q_k = Q_{k-1}q_k + Q_{k-2}$$

obtenidas antes para fracciones continuas finitas, son válidas también para fracciones continuas infinitas, ya que durante la deducción de estas relaciones no hemos considerado, en ninguna parte, que la fracción continua es finita. Por consiguiente, también se conserva la relación (2.7) entre fracciones reducidas consecutivas :

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \tag{4.5}$$

Así, por ejemplo, para las fracciones reducidas, obtenidas al desarrollar $\sqrt{2}$ en fracción continua, siendo $k = 3$ y $k = 4$, conforme a las fórmulas (4.3), tendremos:

$$\delta_3 - \delta_2 = \frac{7}{5} - \frac{3}{2} = \frac{-1}{10},$$
$$\delta_4 - \delta_3 = \frac{17}{12} - \frac{7}{5} = \frac{1}{60},$$

lo que, naturalmente, coincide con el resultado indicado en la relación (4.5).

De la relación (4.5), en particular, se deduce que

$$\delta_{2k} - \delta_{2k+1} = -(\delta_{2k+1} - \delta_2 k) = -\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}} = \frac{1}{Q_{2k+a}Q_{2k}}.$$

Demostremos ahora que es justa la desigualdad:

$$0 < P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}. \tag{4.6}$$

En efecto, el primer miembro de esta desigualdad se obtiene inmediatamente, puesto que conforme a las desigualdades (4.4)

$$\alpha < \delta_{2k} = \frac{P_{2k}}{Q_{2k}}; \quad \alpha Q_{2k}; \quad 0 < P_{2k} - \alpha Q_{2k}.$$

La demostración del segundo miembro de la desigualdad (4.6) es también fácil. Conforme a las desigualdades (4.4)

$$\delta_{2k+1} < \alpha < \delta_{2k},$$

por consiguiente,

$$\delta_{2k}\alpha < \delta_{2k}\delta_{2k+1} = \frac{1}{Q_{2k}Q_{2k+1}}.$$

De aquí, sustituyendo δ_{2k} por $\dfrac{P_{2k}}{Q_{2k}}$, tenemos:

$$\frac{P_{2k}}{Q_{2k}} - \alpha < \frac{1}{Q_{2k}Q_{2k+1}}$$

Multiplicando esta desigualdad por Q_{2k}, obtenemos el resultado pedido:

$$P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k-1}}.$$

Apliquemos los resultados obtenidos para resolver la ecuación

$$x^2 - 2y^2 = 1. \tag{4.7}$$

Transformamos el primer miembro de esta ecuación:

$$x^2 - 2y^2 = \left(x - \sqrt{2}y\right)\left(x + \sqrt{2}y\right).$$

Consideramos que $x = P_{2k}$ e $y = Q_{2k}$, siendo P_{2k} y Q_{2k} numerador y denominador de la correspondiente fracción reducida del desarrollo de $\sqrt{2}$ en fracción continua. Entonces

$$P_{2k}^2 - 2Q_{2k}^2 = \left(P_{2k} - \sqrt{2}Q_{2k}\right)\left(P_{2k} + \sqrt{2}Q_{2k}\right). \tag{4.8}$$

El primer miembro de la igualdad obtenida y, por consiguiente, también el segundo es número entero. Demostremos que este número entero es mayor que cero, pero menor que dos y, por lo tanto, es igual a la unidad. Para ello utilizamos la desigualdad (4.6) siendo $a = \sqrt{2}$:

$$0 < P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}}. \tag{4.9}$$

De aquí observamos que los dos factores en el segundo miembro de (4.8) son positivos y por lo tanto,

$$P_{2k}^2 - 2Q_{2k}^2 > 0.$$

Por otra parte,

$$P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}} = \frac{1}{Q_{2k}q_{2k} + Q_{2k-1}} = \frac{1}{2Q_{2k} + Q_{2k-1}} < \frac{1}{2Q_{2k}}$$

Pero, conforme a la fórmula (4.4),

$$\delta_{2k} = \frac{P_{2k}}{Q_{2k}} > \sqrt{2}$$

y por consiguiente

$$\sqrt{2}Q_{2k} < P_{2k},$$
$$P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k},$$

así obtenemos dos desigualdades para los factores del segundo miembro de la igualdad (4.8), o sea:

$$P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{2Q_{2k}},$$

$$P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}.$$

Al multiplicar estas dos desigualdades resulta :

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}}.$$

De aquí, utilizando la desigualdad (4.9), obtenemos:

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{\sqrt{2}Q_{2k} + \dfrac{1}{Q_{2k+1}}}{Q_{2k}} = \sqrt{2} + \frac{1}{Q_{2k}Q_{2k+1}}$$

pero como para todos los $k \geqslant 1$

$$\frac{1}{Q_{2k}Q_{2k+1}} \leqslant \frac{1}{Q_2 Q_3} = \frac{1}{10}$$

entonces

$$P_{2k}^2 - 2Q_{2k}^2 < \sqrt{2} + \frac{1}{10} < 2.$$

Así, pues, hemos demostrado que el número entero de $P_{2k}^2 - 2Q_{2k}^2$ para cualquier $k \geqslant 1$, verifica las desigualdades

$$0 < P_{2k}^2 - 2Q_{2k}^2 < 2$$

y, por lo tanto,

$$P_{22}^2 - 2Q_{2k}^2 = 1,$$

es decir, $x = P_{2k}$ e $y = Q_{2k}$ para cualquier $k \geqslant 1$ dan solución a la ecuación

$$x^2 - 2y^2 = 1.$$

De momento no sabemos si las soluciones halladas para la ecuación (4.7) son, o no, todas las soluciones de esta ecuación.

Ahora surge ya lógicamente la pregunta cómo obtener todas las soluciones en números enteros x e y de la ecuación

$$x^2 - Ay^2 = 1, \tag{4.10}$$

siendo $A > 0$ un número entero y $\sqrt{A}$ un número irracional. Demostraremos que esto es posible si se conoce al menos una solución de la ecuación (4.10). A base de la ecuación (4.7) hemos comprobado que ecuaciones como ésta tienen solución. Examinemos, a continuación, el problema de cómo obtener todas las soluciones de la ecuación (4.10) a partir de una determinada, la cual llamaremos solución mínima dejando por el momento de lado la pregunta de si la ecuación (4.10) tiene siempre, por lo menos, una solución en números enteros diferente a la trivial $x = 1, y = 0$.

Supongamos que la ecuación (4.10) tiene solución no trivial $[x_0, y_0]$, $x_0 > 0$, $y_0 > 0$ y

$$x_0^2 - Ay_0^2 = 1. \tag{4.11}$$

(Recordemos que solución se llama un par de números enteros $[x_0, y_0]$ el cual verifica una ecuación.) Llamaremos a esta solución $[x_0, y_0]$ *mínima* si, siendo $x = x_0$ e $y = y_0$, el binomio $x + \sqrt{A}y$, ($\sqrt{A} > 0$) adquiere el menor valor posible entre todos los valores que puede adquirir al sustituir x e y por todas las posibles soluciones positivas (diferentes de 0) de la ecuación (4.10). Por ejemplo, solución mínima de la ecuación (4.7) será $x = 3$ e $y = 2$, ya que la expresión $x + \sqrt{2}y$, para estos valores de x e y, adquiere el valor $3 + 2\sqrt{2}$; la ecuación (4.7) no tiene otra solución, lo que es fácil comprobar seleccionando números pequeños enteros positivos que puedan ser la solución que da al binomio $x + \sqrt{2}y$ un valor no superior a $3 + 2\sqrt{2}$. Efectivamente la siguiente solución de la ecuación (4.7), por su valor, es $x = 17$ e $y = 12$. Claro está que $17 + 12\sqrt{2}$ es mayor que $3 + 2\sqrt{2}$. Observaremos también que *no existen dos soluciones mínimas de la ecuación (4.10)*. Admitiendo lo contrario, es decir, que existen dos soluciones, $[x_1, y_1]$ y $[x_2, y_2]$, que dan un mismo valor al binomio $x + \sqrt{A}y$, tendremos que:

$$x_1\sqrt{A}y_1 + = x_2 + \sqrt{A}y_2 \tag{4.12}$$

Pero, como $\sqrt{A}$ es irracional y $x_1 y_1, x_2, y_2$ son números enteros, de la igualdad (4.12) se deduce directamente que

$$x_1 - x_2 = (y_2 - y_1)\sqrt{A},$$

lo que no es posible puesto que $x_1 - x_2$ es un número entero mientras que $(y_2 - y_1)\sqrt{A}$, por ser la multiplicación de un número entero por un irracional, es número irracional, y un número entero no puede ser número irracional. Esta contradicción desaparece cuando $x_1 = x_2$ e $y_1 = y_2$, es decir, cuando no operarnos con dos distintas soluciones sino con una. O sea, de existir solución mínima, ésta es única. Analicemos otra propiedad muy importante de las soluciones de la ecuación (4.10). Sea $[x_1, y_1]$

solución de la ecuación (4.10). Entonces

$$x_1^2 - Ay_1^2 = 1,$$

o bien

$$\left(x_1 + \sqrt{A}y_1\right)\left(x1 - \sqrt{A}y_1\right) = 1. \tag{4.13}$$

Elevemos los dos miembros de la igualdad (4.13) a la potencia n entera y positiva:

$$\left(x_1 + \sqrt{A}y_1\right)^n \left(x_1 - \sqrt{A}y_1\right)^n = 1. \tag{4.14}$$

Elevando a potencia conforme a la fórmula del binomio de Newton, obtenemos:

$$\left(x_1 + \sqrt{A}y_1\right)^n = x_1^n + nx_1^{n-1}\sqrt{A}y_1 + \\ + \frac{n(n-1)}{2}x_1^{n-2}Ay_1^2 + \cdots + (\sqrt{A})^n y_1^n = x_n + \sqrt{A}y_n, \tag{4.15}$$

aquí x_n e y_n son números enteros, ya que el primero, tercero y, en general, todos los términos impares del desarrollo por la fórmula del binomio son números enteros; los términos pares son números enteros multiplicados por $\sqrt{A}$. Agrupando por separado sumas enteras y números múltiplos de $\sqrt{A}$, obtenemos la igualdad (4.15). Los números x_n e y_n, como demostraremos a continuación, también son solución de la ecuación (4.10). En efecto, sustituyendo el signo de $\sqrt{A}$ en la igualdad (4.15), obtenemos la siguiente igualdad

$$\left(x_1 - \sqrt{A}y_1\right)^n = x_n - \sqrt{A}y_n. \tag{4.16}$$

Multiplicando las igualdades (4.15) y (4.16) término por término, y valiéndonos de la igualdad (4.14), finalmente tendremos:

$$\left(x_1 + \sqrt{A}y_1\right)^n \left(x_1 - \sqrt{A}y_1\right)^n = \\ = \left(x_n + \sqrt{A}y_n\right)\left(x_n - \sqrt{A}y_n\right) = x_n^2 - Ay_n^2 = 1, \tag{4.17}$$

o sea, $[x_n, y_n]$ es *también solución de la ecuación* (4.10).

Ahora podemos ya demostrar el teorema fundamental relacionado con las soluciones de la ecuación (4.10).

4.0.1 Teorema: Cualquier solución de la ecuación (4.10)

$$x^2 - Ay^2 = 1,$$

siendo A un número positivo y $\sqrt{A}$ un número la forma $[\pm x_n, \pm y_n]$, en la que

$$\left.\begin{aligned} x_n &= \frac{1}{2}\left[\left(x_0 + y_0\sqrt{A}\right)^n + \left(x_0 - y_0\sqrt{A}\right)^n\right], \\ y_n &= \frac{1}{2\sqrt{A}}\left[\left(x_0 + y_0\sqrt{A}\right)^n - \left(x_0 - y_0\sqrt{A}\right)^n\right], \end{aligned}\right\} \tag{4.18}$$

y $[x_0, y_0]$ es la solución mínima.

DEMOSTRACIÓN: Supongamos lo contrario, que existe una solución $[x', y']$ de la ecuación (4.10) en números enteros positivos tal, que la igualdad

$$x' + \sqrt{A}y' = \left(x_0 + \sqrt{A}y_0\right)^n \tag{4.19}$$

no es justa para ningún número entero y positivo n. Analicemos la serie de números

$$x_0 + \sqrt{A}y_0, \quad \left(x_0 + \sqrt{A}y_0\right)^2, \quad \left(x_0 + \sqrt{A}y_0\right)^3, \ldots$$

Esta es una serie de números positivos que crecen ilimitadamente ya que $x_0 \geqslant 1$, $y_0 \geqslant 1$ y $x_0 + \sqrt{A}y_0 > 1$. Puesto que $[x_0, y_0]$ es solución mínima, conforme a la determinación de solución mínima, tenemos

$$x' + \sqrt{A}y' > x_0 + \sqrt{A}y_0$$

Por lo tanto, siempre se puede hallar un número entero $n \geqslant 1$ con el cual

$$\left(x_0 + \sqrt{A}y_0\right)^n < x' + \sqrt{A}y' < \left(x_0 + \sqrt{A}y_0\right)^{n+1} \tag{4.20}$$

Pero, $x_0 - \sqrt{A}y_0 > 0$ puesto que

$$\left(x_0 + \sqrt{A}y_0\right)\left(x_0 - \sqrt{A}y_0\right) = x_0^2 - Ay_0^2 = 1 > 0.$$

Por consiguiente la multiplicación de todos los términos de las desigualdades (4.20)

por un mismo número positivo $\left(x_0 - \sqrt{A}y_0\right)^n$ no cambia los signos de estas desigualdades y por lo tanto tendremos:

$$\left(x_0 + \sqrt{A}y_0\right)^n \left(x_0 - \sqrt{A}y_0\right)^n < \left(x' + \sqrt{A}y'\right) \left(x_0 - -\sqrt{A}y_0\right)^n < \\ < \left(x_0 + \sqrt{A}y_0\right)^n \left(x_0 - \sqrt{A}y_0\right)^n . \quad (4.21)$$

Puesto que

$$\left(x_0 + \sqrt{A}y_0\right)^n \left(x_0 - \sqrt{A}y_0\right)^n = \left(x_0^2 - Ay_0^2\right)^n = 1, \quad (4.22)$$

entonces

$$\left(x_0 + \sqrt{A}y_0\right)^{n+1} \left(x_0 - \sqrt{A}y_0\right)^n = x_0 - \sqrt{A}y_0 = 1. \quad (4.23)$$

Además

$$\left(x' + \sqrt{A}y'\right) \left(x_0 - \sqrt{A}y_0\right)^n = \left(x' + \sqrt{A}y'\right) \left(x_n - \sqrt{A}y_n\right) = \\ = x'x_n - Ay'y_n + \sqrt{A}\left(y'x_n - x'y_n\right) = \overline{x} + \sqrt{A}\overline{y}, \quad (4.24)$$

siendo aquí x e y números enteros y

$$x_n - \sqrt{A}y_n = \left(x_0 - \sqrt{A}y_0\right)^n .$$

Valiéndonos de las relaciones de (4.22) a (4.24) y de las desigualdades (4.21), obtenemos la desigualdad:

$$1 < \overline{x} + \sqrt{A}\overline{y} < x_0 + \sqrt{A}y_0 \quad (4.25)$$

Demostremos que el par de números enteros $\overline{x}$ e $\overline{y}$ es solución de la ecuación (4.10). En efecto, multiplicando la igualdad (4.24) término por término, o sea la igualdad

$$\overline{x} + \sqrt{A}\overline{y} = \left(x' + \sqrt{A}y'\right) \left(x_0 - \sqrt{A}y_0\right)^n , \quad (4.26)$$

por la igualdad

$$\overline{x} - \sqrt{A}\overline{y} = \left(x' - \sqrt{A}y'\right) \left(x_0 + \sqrt{A}y_0\right) , \quad (4.27)$$

obtenida directamente de la (4.24) cambiando el signo de $\sqrt{A}$, tendremos

$$\left(\overline{x} + \sqrt{A}\overline{y}\right)\left(\overline{x} - \sqrt{A}\overline{y}\right) = \overline{x}^2 - A\overline{y}^2 =$$
$$= \left(x' + \sqrt{A}y'\right)\left(x' - \sqrt{A}y'\right)\left(x_0 + \sqrt{A}y_0\right)^n\left(x_0 - \sqrt{A}y_0\right)^n =$$
$$\left(x'^2 - Ay'^2\right)\left(x_0^2 - Ay_0^2\right) = 1, \quad (4.28)$$

ya que $[x', y']$ y $[x_0, y_0]$ son soluciones de la ecuación (4.10). Por último demostraremos que $\overline{x} > 0$ e $\overline{y} > 0$. Ante todo, está claro que $\overline{x}$ no es igual a cero. En efecto, si $\overline{x} = 0$, a base de la igualdad (4.28) hallamos que

$$-Ay_0^2 = 1,$$

lo cual es imposible puesto que $A > 0$. Por otra parte, si $y = 0$, entonces $x^2 = 1$ lo cual tampoco es posible puesto que, conforme a la desigualdad (4.25), $\overline{x} > 1$. Observaremos, por último, que los signos de $\overline{x}$ e $\overline{y}$ deben ser iguales. En efecto, suponiendo que los signos de $\overline{x}$ e $\overline{y}$ son diferentes, los signos de $\overline{x}$ e $-\overline{y}$ lógicamente deben ser iguales. Y entonces, comparando los valores absolutos de las expresiones $\overline{x} + \sqrt{A}\overline{y}$ y $\overline{x} - \sqrt{A}\overline{y}$, resulta que el valor absoluto de la primera expresión es menor que el valor absoluto de la segunda, ya que en la primera los dos números con signos iguales se restan uno del otro mientras que en la segunda se suman. Mas, sabemos que

$$\overline{x} + \sqrt{A}\overline{y} > 1$$

y, por lo tanto, $\overline{x} - \sqrt{A}\overline{y}$, en valor absoluto, también es mayor que 1. Pero,

$$\left(\overline{x} + \sqrt{A}\overline{y}\right)\left(\overline{x} - \sqrt{A}\overline{y}\right) = \overline{x}^2 - Ay^2 = 1,$$

lo que nos conduce a una contradicción pues la multiplicación de dos números, cada uno de los cuales tiene un valor absoluto mayor que la unidad, debe tener también un valor absoluto mayor que la unidad. Por lo tanto, los signos de $\overline{x}$ e $\overline{y}$ son iguales y $\overline{x} \neq 0$ e $\overline{y} \neq 0$. Ahora bien, de la desigualdad (4.25) inmediatamente se deduce que $\overline{x} > 0$ e $\overline{y} > 0$. Suponiendo que existe una solución $[x', y']$ de la ecuación

$$x^2 - Ay^2 = 1, \qquad A > 0,$$

tal que la igualdad (4.19) no es posible con ningún número entero y positivo n, hemos conseguido determinar una solución $[\overline{x}, \overline{y}]$ de esta ecuación, siendo $\overline{x} > 0, \overline{y} > 0$

y $\overline{x}$ e $\overline{y}$ números enteros, la cual satisface las desigualdades (4.25) que contradicen la definición dada a la solución mínima $[x_0, y_0]$. Con ello hemos demostrado que la suposición de que existe una solución no dada por la fórmula (4.19), nos lleva a una contradicción. En otras palabras, hemos demostrado que todas las soluciones de nuestra ecuación pueden ser obtenidas a base de la fórmula (4.19).

Así, pues, cualquier solución $[x, y]$ de la ecuación (4.10) se obtiene mediante la relación:

$$x + y\sqrt{A}y = \left(x_0 + \sqrt{A}y_0\right)^n \quad n \geqslant 0, \tag{4.29}$$

siendo $[x_0, y_0]$ solución mínima. Cambiando en esta última igualdad el signo de $\sqrt{A}$, obtendremos también una igualdad:

$$x - \sqrt{A}y = \left(x_0 - \sqrt{A}y_0\right)^n. \tag{4.30}$$

Sumando y restando estas igualdades y dividiendo ambos miembros por 2 ó $2\sqrt{A}$, respectivamente, obtenemos:

$$\left.\begin{aligned} x = x_n &= \frac{1}{2}\left[\left(x_0 + \sqrt{A}y_0\right)^n + \left(x_0 - \sqrt{A}y_0\right)^n\right], \\ y = y_n &= \frac{1}{2\sqrt{A}}\left[\left(x_0 + \sqrt{A}y_0\right)^n - \left(x_0 - \sqrt{A}y_0\right)^n\right], \end{aligned}\right\} \tag{4.31}$$

es decir, expresiones explícitas para cualquier solución $[x, y]$, siendo x e y números positivos. Cualquier solución puede obtenerse de las ecuaciones (4.31) tomando arbitrariamente los signos para x_n e y_n. □

Por ejemplo, como ya hemos visto anteriormente solución mínima de la ecuación $x^2 - 2y^2 = 1$ es $x = 3$ e $y = 2$, por lo tanto, todas las soluciones de esta ecuación estarán incluidas en las fórmulas:

$$x_n = \frac{1}{2}\left[\left(3 + 2\sqrt{2}\right)^n + \left(3 - 2\sqrt{2}\right)^n\right].$$

$$y = \frac{1}{2\sqrt{2}}\left[\left(3 + 2\sqrt{2}\right)^n - \left(3 - 2\sqrt{2}\right)^n\right],$$

a base de ellas, siendo $n = 1, 2, 3$, obtenemos las soluciones: $[3, 2]$, $[17, 12]$, $[99, 70]$.

Observemos que los números x_n e y_n al crecer n, crecen a la velocidad de una progresión geométrica cuyo denominador es $x_0 + \sqrt{A}y_0$; puesto que, basándonos en la igualdad

$$\left(x_0 + \sqrt{A}y_0\right)\left(x_0 - \sqrt{A}y_0\right) = 1,$$

podemos afirmar que

$$0 < x_0 \sqrt{A} y_0 < 1$$

y, por consiguiente, $\left(x_0 - \sqrt{A} y_0\right)^n$ siempre tiende a cero al crecer n.

Ahora podemos ver que si la ecuación (4.10) tiene por lo menos una solución no trivial (aunque sea una solución para $y \neq 0$), entonces esta ecuación también tendrá solución mínima y, por consiguiente, todas sus demás soluciones pueden ser halladas empleando las fórmulas (4.31). Volvamos ahora a la cuestión de si existe o no, para esta ecuación, solución no trivial cuando $\sqrt{A}$ es un valor arbitrario entero y positivo y $\sqrt{A}$, un valor irracional

CAPÍTULO 5

Caso general para ecuaciones de segundo grado con dos incógnitas

En este párrafo demostraremos que, para cualesquiera números positivo A e irracional $\sqrt{A}$, la ecuación

$$x^2 - Ay^2 = 1 \tag{5.1}$$

siempre tiene solución no trivial, es decir, existe un par de números enteros x_0 e y_0 $(x_0, y_0 \neq 0)$ que satisface esta ecuación. Veamos, primeramente, el procedimiento utilizado para desarrollar en fracción continua un número positivo arbitrario. Anteriormente, para desarrollar en fracción continua, nos hemos valido de las propiedades especificas del número $\sqrt{2}$. Sea α un número positivo cualquiera. Entonces siempre existe un número entero menor o igual que α y mayor que $\alpha - 1$. Este número entero se llama *parte entera* de α y se designa por $[\alpha]$. La diferencia entre α y su parte entera se llama *parte fraccionaria del número* α y se designa por $\{\alpha\}$. De las definiciones de parte entera y parte fraccionaria del número α se deduce directamente la relación entre ambas, o sea:

$$\alpha - [\alpha] = \{\alpha\}$$

o bien

$$\alpha = [\alpha] + \{\alpha\}. \tag{5.2}$$

Puesto que parte fraccionaria de un número es la diferencia entre un número positivo y un número entero máximo, no superior a dicho número positivo, la parte fraccionaria de un número es siempre menor que la unidad y no negativa. Por ejemplo, la parte

entera de $\frac{27}{5}$ es 5 y parte y la parte fraccionaria, $\frac{2}{5}$; la parte entera de $\sqrt{2}$ es 1 y la parte fraccionaria, $\sqrt{2} - 1$; la parte entera de $\sqrt[3]{52}$ es igual a 3 y la parte fraccionaria, igual a $\sqrt[3]{52} - 3$ etc.

La definición que hemos hecho de parte entera y parte fraccionaria de un número positivo α puede ser utilizada para desarrollar este número en fracción continua. Supongamos que:

$$[\alpha] = q_1, \quad \{\alpha\} = \frac{1}{\alpha_1}.$$

Entonces

$$\alpha = q_1 + \frac{1}{\alpha_1} \tag{5.3}$$

Como $\{\alpha\}$ es siempre menor que la unidad, entonces α_1 será siempre mayor que la unidad. Sí α fuese número entero, entonces su parte fraccionaria sería igual a cero y α_1 sería igual a la infinidad, por eso, tendríamos la igualdad $\alpha = q_1$. Abstrayéndonos de este caso particular, el cual se excluye puesto que el número que desarrollamos en fracción continua es irracional, podemos afirmar que α_1 es un número positivo mayor que la unidad. Con α_1 procedemos lo mismo que con α, y escribimos la igualdad

$$\alpha_1 = q_2 + \frac{1}{\alpha_2} \quad q_2 = [\alpha_1], \quad \frac{1}{\alpha_2} = \{\alpha_1\}.$$

Continuando este procedimiento, obtenemos una serie de ecuaciones:

$$\left.\begin{array}{r} \alpha = q_1 + \frac{1}{\alpha_1}, \quad q_1 = [\alpha], \\ \alpha_1 = q_2 + \frac{1}{\alpha_2}, \quad q_2 = [\alpha_1], \\ \alpha_2 = q_3 + \frac{1}{\alpha_3}, \quad q_3 = [\alpha_2], \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_{n-1} = q_n + \frac{1}{\alpha_n}, \quad q_n = [\alpha_{n-1}], \\ \dots\dots\dots\dots\dots\dots\dots\dots \end{array}\right\} \tag{5.4}$$

No es difícil comprobar que el procedimiento utilizado para obtener una sucesión de números enteros $q_1, \ \dots, \ q_n$, cuando $\alpha\frac{a}{b}$ es un número racional, es decir, cuando $\alpha = \frac{a}{b}$ siendo a y b números enteros y positivos, no se diferencia por sus resultados del procedimiento utilizado para obtener cocientes incompletos mediante el algoritmo de Euclides (véanse las fórmulas (2.5)). Por eso, para a racional, este procedimiento debe interrumpirse . Cuando α es irracional dicho procedimiento debe ser

infinito. En efecto, si para algún n α_n fuese número entero, entonces α_{n-1} sería número racional, lo que a su vez conduciría a la racionalidad de α_{n-2} y así sucesivamente hasta obtener la racionalidad de α_1. De las fórmulas (5.4), realizando sustituciones consecutivas y excluyendo α_1, ..., α_{n-1} obtenemos la siguiente fracción continua:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n + \cfrac{1}{\alpha_n}}}} \tag{5.5}$$

la cual también puede expresarse en forma de fracción continua infinita, puesto que n puede tomarse tan grande como se quiera, es decir

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n + \cdots}}}$$

Como ya hemos indicado en el párrafo 4, en este caso, la relación (2.7) entre fracciones reducidas se mantiene puesto que no depende del carácter finito o infinito de la fracción. De la relación (2.7), como hemos observado, se deduce la desigualdad (4.6) para fracciones reducidas pares. Esta desigualdad (4.6) se toma nuevamente como base para demostrar la existencia de solución de la ecuación (5.1), pero dicha demostración es más complicada que para el caso particular cuando $A = 2$. Si el lector desea conocer más a fondo la teoría de las fracciones continuas, le recomendamos el libro de A. Ya. Jinchin «Fracciones continuas».

5.0.1 Teorema: Para cualquier entero positivo A e irracional $\sqrt{A}$, la ecuación (5.1)

$$x^2 - Ay^2 = 1,$$

tiene solución no trivial $[x_0, y_0]$, $x_0 > 0, y_0 > 0$.

Demostración: Puesto que esta demostración es algo complicada, conviene dividirla en una serie de etapas. La primera etapa consiste en demostrar la existencia de un número k entero positivo, cuyas propiedades hacen que la igualdad

$$x^2 - Ay^2 = k \tag{5.6}$$

tenga una infinidad de soluciones en números enteros positivos x e y. En efecto, examinemos el binomio $x^2 - Ay^2$. Sustituyendo en él x e y por los numeradores y

denominadores de las fracciones reducidas pares, obtenidas consecutivamente desarrollando el número irracional $\alpha = \sqrt{A}$, tendremos

$$z_{2n} = P_{2n}^2 - AQ_{2n}^2 = (P_{2n} - \alpha Q_{2n})(P_{2n} + \alpha Q_{2n}). \tag{5.7}$$

Pero como

$$0 < P_{2n} - \alpha Q_{2n} < \frac{1}{Q_{2n+1}},$$

se deduce directamente que:

$$0 < P_{2n} + \alpha Q_{2n} = 2\alpha Q_{2n} + P_{2n} - \alpha Q_{2n} < 2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}.$$

Utilicemos estas dos últimas desigualdades para valorar z_{2n}. Sustituyendo, mediante estas desigualdades, los dos factores en el segundo miembro de la igualdad (5.7) por magnitudes mayores, obtenemos para z_{2n} la desigualdad:

$$0 < z_{2n} < \frac{1}{Q_{2n+1}}\left(2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}\right) < 2\alpha + 1, \tag{5.8}$$

puesto que Q_{2n} es menor que Q_{2n+1}. Sustituyendo en el binomio

$$z = x^2 - Ay^2$$

x e y por P_{2n} y Q_{2n}, respectivamente, z adquiere un valor entero positivo. Resulta, pues, que todos los números $z_2, z_4, ..., z_{2n}, ...$ son enteros positivos que no superan un mismo número $2\alpha + 1$. Pero como $\alpha = \sqrt{A}$ es irracional, la fracción continua será infinita y, por consiguiente, la cantidad de pares, P_{2n} y Q_{2n}, será infinitamente grande. Entre los números enteros positivos $z_2, z_4, ..., z_{2n}, ...$ diferentes habrá solamente una cantidad finita, ya que entre 1 y $2\alpha + 1$, siendo este último completamente definido e independiente de n, no puede haber más de $[2\alpha + 1]$ números enteros. O sea, la serie infinita de números $z_2, z_4, ..., z_{2n}, ...$ no es otra cosa que una sucesión de números enteros 1, 2, 3, ..., $[2\alpha + 1]$ que se repiten de algún modo; además, incluso no es obligatorio que todos estos números se encuentren en la sucesión $z_2, z_4, z_6, ...$ Como la sucesión $z_2, z_4, ..., z_{2n}, ...$ es infinita mientras que la cantidad de sus diferentes términos es finita, por lo menos un número k $(1 \leqslant k \leqslant [2\alpha + 1])$ se repite en esta sucesión multitud infinita de veces. Es decir, entre los pares de números $[P_2, Q_2]$, $[P_4, Q_4]$, ..., $[P_{2n}, Q_{2n}]$, ... hay una multitud infinita de pares, tales, que sustituyendo por ellos x e y, la expresión $z = x^2 - Ay^2$ adquiere siempre un mismo valor k. Así, pues, hemos demostrado la existencia de un número entero positivo k, con el cual la ecuación (5.6) tiene infinidad de soluciones en números enteros x e y. Enumeremos

de nuevo estos pares de números, válidos como soluciones de la ecuación (5.6) para k determinado designándolos por $[u_1, v_1]$, $[u_2, v_2]$, ..., $[u_n, v_n]$, ... Tendremos entonces que

$$u_n^2 - Av_n^2 = k. \tag{5.9}$$

Observaremos que la sucesión de pares $[u_1, v_1]$, $[u_2, v_2]$, ..., $[u_n, v_n]$, ... es parte de la sucesión de pares de numeradores y denominadores de las fracciones reducidas pares del número α. Si pudiésemos afirmar que $k = 1$, con ello quedaría demostrado que la ecuación (5.1) tiene multitud infinita de soluciones en números enteros. Pero como no lo podemos afirmar, vamos a suponer que $k > 1$ (de lo contrario, o sea, siendo $k = 1$ quedará todo demostrado) y así pasaremos a la segunda etapa de nuestra demostración. Demostraremos a continuación, que entre los pares de números enteros $[u_1, v_1]$, ..., $[u_n, v_n]$, ... hay multitud infinita de pares, que al dividirlos por k, dan restos iguales, es decir, que existen dos números enteros no negativos p y q, menores que k, tales, que para la multitud infinita de pares $[u_1, v_1]$, ..., $[u_n, v_n]$ son verídicas las igualdades:

$$u_n = a_nk + p \quad \text{y} \quad v_n = b_nk + q, \tag{5.10}$$

donde a_n y b_n son cocientes de la división de u_n y v_n por k, y p, q los restos de esta división. En efecto, si dividimos u_n y v_n por el número entero k, $k > 1$, obtendremos una relación semejante a la (5.10), en la que los restos de la división, como siempre, se hallarán entre 0 y $k - 1$. Como restos de la división de u_n y v_n por k pueden ser, en ambos casos, solamente los números 0, 1, 2,..., $k - 1$, la cantidad posible de pares de restos, dados por la división de u_n y v_n por k, será $k \cdot k = k^2$. Esto también queda claro si tenemos en cuenta que a cada par $[u_n, v_n]$ corresponde un par de restos $[p_n, q_n]$, además p_n y q_n no pueden adquirir, cada uno por separado, más de k valores diferentes, por eso, la cantidad de pares será no superior a k^2. O sea, a cada par de números enteros $[u_n, v_n]$ corresponde un par de restos $[p_n, q_n]$ al ser divididos por k. Pero la cantidad de distintos pares de restos es finita y no supera k^2 mientras que la cantidad de pares $[u_n, v_n]$ es infinita. Entonces, como la serie de pares $[p_1, q_1]$, $[p_2, q_2]$, ..., $[p_n, q_n]$, ... tiene solamente una cantidad finita de distintos pares, por lo menos, un par se repite multitud infinita de veces. Designando este par de restos por $[p, q]$, determinamos que existe una multitud infinita de pares $[u_n, v_n]$ los cuales satisfacen tas igualdades (5.10). Ya que para algunos valores determinados de p y q, cuya existencia acabamos de demostrar, no todos los pares $[u_n, v_n]$ satisfacen tas igualdades (5.10), volvemos de nuevo a enumerar todos aquellos pares $[u_n, v_n]$ que satisfacen dichas igualdades designándolos por $[R_n, S_n]$. Entonces, la sucesión infinita de pares $[R_1, S_1]$, $[R_2, S_2]$, ..., $[R_n, S_n]$, ... es parte de la sucesión de pares $[u_n, v_n]$, la cual a su vez, es parte de la sucesión de pares de numeradores y denominadores de las fracciones reducidas pares de α. Los pares de números de esta sucesión verifican la

ecuación (5.9) y dan los mismos restos p y q al ser divididos por k.

Ahora, cuando hemos establecido la existencia de una multitud infinita de tales pares de números enteros positivos R_n, S_n, podemos pasar a la tercera y última etapa de nuestra demostración.

Ante todo, indicaremos que los pares $[R_n, S_n]$, siendo pares de numeradores y denominadores de fracciones reducidas, deben ser pares de números primos entre sí. es decir, no deben tener divisores comunes. En efecto, si cambiamos en la relación (4.5) k por $2k$ y consideramos que $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}$ y $\delta_{2k-1} = \frac{P_{2k-1}}{Q_{2k-1}}$, entonces de la relación

$$\frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}} = \frac{1}{Q_{2k}Q_{2k-1}}$$

multiplicando sus dos miembros por $Q_{2k}Q_{2k-1}$, obtenemos la igualdad

$$P_{2k}Q_{2k-1} - Q_{2k}P_{2k-1} = 1. \tag{5.11}$$

La relación entre números enteros P_{2k} Q_{2k}, $P - 2k - 1$ y Q_{2k-1} demuestra que teniendo P_{2k} y Q_{2k} un divisor común mayor que la unidad, el primer miembro de esta relación debe ser divisible por este mismo divisor común. Pero el segundo miembro de la igualdad es igual a la unidad que no es divisible por ningún número mayor que 1. Así, pues, queda demostrado que los números R_n y S_n, los cuales pueden ser solamente numeradores y denominadores de fracciones reducidas, son primos entre sí. De la relación (2.6) también se deduce directamente que

$$Q_2 < Q_4 < \cdots < Q_{2n} < \cdots$$

Como los números R_n y S_n son primos entre sí y los números S_1, ..., S_n, ... diferentes entre sí por ser tomados de una sucesión de números Q_{2n} también diferentes entre sí, se deduce directamente que en la serie infinita de fracciones

$$\frac{R_1}{S_1}, \frac{R_2}{S_2}, \ldots \frac{R_n}{S_n} \ldots$$

no hay números iguales. Veamos las dos siguientes igualdades, deducidas de la definición de los números R_n y S_n, o sea:

$$R_1^2 - AS_1^2 = (R_1 - \alpha S_1)(R_1 + \alpha S_1) = k \tag{5.12}$$

y

$$R_2^2 - AS_2^2 = (R_2 - \alpha S_2)(R_2^2 + \alpha S_2) = k, \tag{5.13}$$

donde sigue siendo $\alpha = \sqrt{A}$.

A continuación, tenemos

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = R_1R_2 - AS_1S_2 + \alpha(R_1S_2 - S_1R_2), \tag{5.14}$$

puesto que $\alpha^2 = A$, y de igual forma

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = R_1R_2 - AS_1S_2 - \alpha(R_1S_2 - S_1R_2). \tag{5.15}$$

Pero como al ser divididos por kR_n y S_n dan restos iguales que no dependen de n, en virtud de la relación (5.10), tenemos:

$$R_n = c_nk + p \quad \text{y} \quad S_n = d_nk + q. \tag{5.16}$$

Por eso, mediante transformaciones y sustituciones sencillas obtenemos las igualdades:

$$\begin{aligned} R_1R_2 - AS_1S_2 &= R_1(c_2k + p) - AS_1(d_2k + q) = \\ &= R_1[(c_2 - c_1)k + c_1k + p] - AS_1[(d_2 - d_1)k + \\ &+ d_1k + q] = R_1[(c_2 - c_1)k + R_1] - AS_1[(d_2 - d_1)k + \\ &+ S_1] = k[R_1(c_2 - c_1) - AS_1(d_2 - d_1)] + R_1^2 - AS_1^2 = \\ &= k[R_1(c_2 - c_1) - AS_1(d_2 - d_1) + 1] = kx_1, \end{aligned} \tag{5.17}$$

siendo x_1 un número entero, puesto que $R_1^2 - AS_1^2 = k$. De la misma forma

$$\begin{aligned} R_1S_2 - S_1R_2 &= \\ &= R_1[(d_2 - d_1)k + d_1k + q] - S_1[(c_2 - c_1)k + \\ &+ c_1k + p] = R_1[(d_2 - d_1)k + S_1] - S_1[(c_2 - c_1)k + \\ &+ R_1] = k[R_1(d_2 - d_1) - S_1(c_2 - c_1)] = ky_1, \end{aligned} \tag{5.18}$$

siendo y_1 también un número entero. Se puede afirmar que y_1 no es igual a cero. En efecto, si $y_1 = 0$, entonces

$$ky_1 - R_1S_2 - R_2S_1 = 0,$$

y de aquí

$$\frac{R_1}{S_1} = \frac{R_2}{S_2}.$$

Esta última igualdad no es posible, ya que hemos constatado que todas las fracciones $\frac{R_n}{S_n}$ son diferentes entre sí. Las igualdades (5.17) y (5.15) demuestran que:

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = kx_1 + \alpha k y_1 = k(x_1 + \alpha y_1) \tag{5.19}$$

y

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = kx_1 - \alpha k y_1 = k(x_1 - \alpha y_1). \tag{5.20}$$

Multiplicando las igualdades (5.12) y (5.13) término por término y utilizando las igualdades (5.19) y (5.20), tendremos:

$$\begin{aligned} k^2 &= (R_1^2 - AS_1^2)(R_2^2 - AS_2^2) = \\ &= (R_1 - \alpha S_1)(R_2 + \alpha S_2)(R_1 + \alpha S_1)(R_2 - \alpha S_2) = \\ &= k^2(x_1 + \alpha y_1)(x_1 - \alpha y_1) = k^2(x_1^2 - Ay_1^2). \end{aligned} \tag{5.21}$$

Simplificando por k^2, obtenemos finalmente:

$$x_1^2 - Ay_1^2 = 1. \tag{5.22}$$

Pero y_1 no es igual a cero, por lo tanto x_1 tampoco puede serlo. De lo contrario, el primer miembro de la ecuación (5.22) sería número negativo y el segundo, igual a uno. Así, pues, incluso suponiendo que k no es igual a uno, hemos encontrado dos números enteros, x_1 e y_1, no iguales a cero, los cuales verifican la ecuación (5.1). Con esto, la teoría de las ecuaciones del tipo (5.1) queda completamente demostrada, pues sabemos que estas ecuaciones, siendo A número entero, $A > 0$, y $\sqrt{A}$, número irracional, siempre tienen solución; y además, mediante la solución mínima, cuya existencia hemos demostrado, podemos hallar todas las soluciones de dichas ecuaciones. □

Prácticamente, la solución mínima se puede hallar seleccionando los valores de x_0 e y_0.

Así, pues, hemos examinado por completo el caso cuando en la ecuación

$$x^2 - Ay^2 = 1$$

$A > 0$ y $\alpha = \sqrt{A}$ es número irracional.

Siendo $A > 0$ y $\alpha = \sqrt{A}$ número entero, esta ecuación puede expresarse de la siguiente forma:

$$x^2 - \alpha^2 y^2 = (x + \alpha y)(x - \alpha y) = 1.$$

y como α es un número entero, entonces siendo x_0 e y_0 números enteros que satisfacen esta ecuación, deberán cumplirse, por separado, las igualdades:

$$x_0 + \alpha y_0 = 1 \quad \text{y} \quad x_0 - \alpha y_0 = 1$$

o las igualdades

$$x_0 + \alpha y_0 = -1 \quad \text{y} \quad x_0 - \alpha y_0 = -1,$$

puesto que la multiplicación de dos números enteros puede ser igual a la unidad si, y sólo si, cada uno de estos números, por separado, es igual a $+1$ o -1. Ambos sistemas de dos ecuaciones con dos incognitas x_0 e y_0 tienen solamente soluciones triviales: $x_0 = 1, y_0 = 0$; $x_0 = -1, y_0 = 0$. *O sea, la ecuación (5.1), siendo A igual al cuadrado de un número entero, tiene solamente soluciones triviales en números enteros $x_0 = \pm 1$, $y_0 = 0$. Las mismas soluciones triviales en números enteros las tiene la ecuación (5.1), siendo A número entero y negativo* (para $A = -1$, hay soluciones triviales simétricas $x_0 = 0, y_0 = \pm 1$).

Examinemos a continuación una ecuación de tipo más general

$$x^2 - Ay^2 = C, \tag{5.23}$$

donde $A > 0$ es número entero; C, número entero y $\alpha = \sqrt{A}$, número irracional. Anteriormente hemos visto que siendo $C = 1$, esta ecuación siempre tiene infinidad de soluciones en números enteros x e y. Siendo C y A valores arbitrarios, estas ecuaciones pueden no tener soluciones en absoluto.

5.0.2 Ejemplo Demostremos que la *ecuación*

$$x^2 - 3y^2 = -1 \tag{5.24}$$

en general no tiene solución en números enteros x e y. Observaremos ante todo, que el cuadrado de un número impar dividido por 8 siempre da como resto 1. En efecto, puesto que cualquier número impar a puede ser expresado como $a = 2N + 1$, siendo N número entero, entonces

$$a^2 = (2N + 1)^2 = 4N^2 + 4N + 1 = 4N(N + 1) + 1 = 8M + 1, \tag{5.25}$$

donde M es número entero, ya que o bien n, o bien $n + 1$ debe ser número par. Además, siendo $[x_0, y_0]$ solución de la ecuación (5.24), x_0 e y_0 no pueden ser números de igual paridad. Si x_0 e y_0 fuesen a la vez pares o impares, entonces, $x_0^2 - 3y_0^2$ sería un número par y no podría ser igual a 1. Si x_0 fuese impar e y_0 par, entonces, la división de x_0^2 por 4 daría 1 de resto, $-3y_0^2$ sería divisible y $x_0^2 - 3y_0^2$ daría 1 de resto. Esto es imposible, ya que al dividir por 4 el segundo miembro da resto trivial -1 o $3 = 4 - 1$. Por último, siendo x_0 par e y_0 impar, x_0^2 es divisible por 4 y $-3y_0^2$, conforme a la expresión (5.25), puede ser dado de la siguiente forma:

$$-3y_0^2 = -3(8M + 1) = -24M - 3 = 4(-6M - 1) + 1$$

y, por lo tanto, dividiendo por 4, tendremos 1 de resto. Por eso, la división de $x_0^2 - 3y_0^2$ por 4 debe dar nuevamente 1 de resto lo que, como ya hemos visto, es imposible. En resumen, no existen números enteros x_0 e y_0, que pueden satisfacer la ecuación (5.24).

No deteniéndonos en el tema sobre cuáles deben ser las cualidades de C y A para que la ecuación (5.23) tenga solución, puesto que este tema es difícil y se resuelve a base de la teoría

general de las irracionalidades cuadráticas de la teoría algebraica de los números, pasaremos al caso en que la ecuación (5.23) tiene solución no trivial. Como en)os casos anteriores, llamaremos solución no trivial $[x', y']$, siendo $x', y' \neq 0$. Admitimos que la ecuación (5.23) tiene solución no trivial $[x', y']$, es decir, admitimos que

$$x'^2 - Ay'^2 = C. \tag{5.26}$$

Manteniendo el mismo valor de A, examinemos la ecuación

$$x^2 - Ay^2 = 1. \tag{5.27}$$

Esta ecuación tiene multitud infinita de soluciones en números enteros, siendo $A > 0$ y $\alpha = \sqrt{A}$ número irracional, y cualquiera de estas soluciones $[\overline{x}, \overline{y}]$ será:

$$\overline{x} = \pm x_n, \quad \overline{y} = \pm y,$$

donde x_n e y_n se determinan por las fórmulas (4.31). Puesto que $[\overline{x}, \overline{y}]$ es solución de la ecuación (5.27), tendremos

$$\overline{x}^2 - A\overline{y}^2 = (\overline{x} + \alpha\overline{y})(\overline{x} - \alpha\overline{y}) = 1.$$

La igualdad (5.26), a su vez, puede ser expresada .de la forma siguiente:

$$(x' + \alpha y')(x' - \alpha y') = C.$$

Multiplicando estas dos últimas igualdades término por término, tendremos.

$$(x' + \alpha y')(\overline{x} + \alpha\overline{y})(x' - \alpha y')(\overline{x} - \alpha\overline{y}) = C. \tag{5.28}$$

Pero

$$(x' + \alpha y')(\overline{x} + \alpha\overline{y}) = x'\overline{x} + Ay'\overline{y} + \alpha(x'\overline{y} + y'\overline{x}).$$

e igualmente

$$(x' - \alpha y')(\overline{x} - \alpha\overline{y}) = x'\overline{x} + Ay'\overline{y} - \alpha(x'\overline{y} + y'\overline{x}).$$

Utilizando estas dos igualdades, podemos expresar la igualdad (5.28) de la forma:

$$[x'\overline{x} + Ay'\overline{y} + \alpha(x'\overline{y} + y'\overline{x})][x'\overline{x} + Ay'\overline{y} - \alpha(x'\overline{y} + y'\overline{x})] = C$$

o de la forma:

$$(x'x + Ay'\overline{y})^2 - A(x'\overline{y} + y'\overline{x})^2 = C.$$

Con esto demostramos que si $[x', y']$ es solución de la ecuación (5.23), esta ecuación será verídica también con el par de números [x,y]:

$$x = x'\overline{x} + Ay'\overline{y}, \quad y = x'\overline{y} + y'\overline{x}, \tag{5.29}$$

siendo $[x, y]$ cualquier solución de la ecuación (5.27). Así, pues, hemos demostrado que *cuando la ecuación (5.23) tiene, por lo menos, una solución, eso significa que tiene multitud infinita de soluciones.*

Claro, no podemos afirmar que las fórmulas (5.29) dan todas las soluciones de la ecuación (5.23). En la teoría de los números algebraicos se demuestra que todas las soluciones de la ecuación (5.23) en números enteros, pueden obtenerse tomando una cantidad de soluciones finita y determinada para esta ecuación, en dependencia de A y C, y propagándolas con ayuda de las fórmulas (5.29). La ecuación (5.23), siendo A valor negativo o igual al cuadrado de un número entero, puede tener solamente una cantidad finita de soluciones. Esto se demuestra con facilidad y, por eso, se lo proponemos hacer a nuestro lector. La resolución, en números enteros, de ecuaciones más generales de segundo grado y con dos incógnitas, del tipo

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0, \tag{5.30}$$

donde A, B, C, D, E y F son números enteros, se reduce mediante sustituciones de las variables, a la resolución de ecuaciones del tipo (5.23), siendo A positivo o negativo. Por eso, el comportamiento de las soluciones de estas ecuaciones, si es que existen, es idéntico al de las soluciones de las ecuaciones del tipo (5.23). Resumiendo podemos constatar que las *ecuaciones de segundo grado con dos incógnitas del tipo (5.30), pueden no tener soluciones en números enteros, pueden tener solamente una cantidad finita de éstas y, por últimn, pueden tener una cantidad infinita de soluciones enteras, las cuales, en este caso, se toman de una cantidad finita de progresiones geométricas generalizadas dadas por las fórmulas (5.29).* Comparando el comportamiento y carácter de las soluciones en números enteros de ecuaciones de segundo grado con dos incógnitas, con el comportamiento de las soluciones de ecuaciones de primer grado, podemos constatar un hecho de suma importancia. O sea, sí las soluciones de una ecuación de primer grado, cuando éstas existen, forman progresiones aritméticas, las soluciones de una ecuación de segundo grado, cuando existe multitud infinita de éstas se toman de una cantidad finita de progresiones geométricas generalizadas. Es decir, pares de números enteros que puedan ser soluciones de una ecuación de segundo grado se encuentran con mucho menos frecuencia que pares de números enteros que puedan ser soluciones de una ecuación de primer grado. Esta circunstancia no es casual. Resulta pues, que las ecuaciones con dos incógnitas y de grado superior al segundo, generalmente, pueden tener sólo una cantidad finita de soluciones. Excepciones a esta regla se dan rara vez.

CAPÍTULO 6

Ecuaciones con dos incógnitas de grado superior al segundo

Las ecuaciones con dos incógnitas de grado superior al segundo, excepto raros casos, pueden tener solamente una cantidad finita de soluciones en números enteros x e y. Analicemos, primeramente, la siguiente ecuación

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2} - y^2 + \cdots + a_ny^n = c, \tag{6.1}$$

donde n es número entero mayor que dos y todos los números $a_0, a_1, \ldots, a_n, c$ son enteros.

Como ya lo demostró a comienzos de nuestro siglo A. Thue, *esta ecuación tiene solamente una cantidad finita de soluciones en números enteros x e y, a excepción, posiblemente, de los casos cuando el primer miembro homogéneo de esta ecuación es potencia de un binomio homogéneo de primer grado o de un trinomio de segundo grado*. En el último caso nuestra ecuación tendrá una de las dos siguientes formas:

$$(ax + by)^n = c_0, \quad (ax^2 + bxy + cy^2)^n = c_0,$$

y, por lo tanto, se convierte en ecuación de primero o segundo grado, ya que para que tenga soluciones, c_0 debe ser n-ésima potencia de un número entero. No podernos en este libro exponer el método de A. Thue, puesto que es complicado y, por eso, nos limitamos a dar algunas explicaciones referentes al carácter de la demostración de que la ecuación (6.1) tiene cantidad finita de soluciones[1].

[1] Este tema se trata, por ejemplo, en el ensayos de A. O. Guelfond «Aproximaciones de números

Dividiendo los dos miembros de la ecuación (6.1) por y^n, ésta tomará la forma:

$$a_0\left(\frac{x}{y}\right)^n + a_1\left(\frac{x}{y}\right)^n + \cdots + a_{n-1}\frac{x}{y} + a_n = \frac{c}{y^n} \tag{6.2}$$

Para facilitar la demostración vamos a suponer, no solamente que todas las raíces de la ecuación

$$a_0z^n + a_1z^{n-1} + \cdots + a_{n-1}z + a_n = 0 \tag{6.3}$$

son distintas y que $a_0a_n \neq 0$, sino también que las raíces de esta ecuación no pueden ser raíces de ecuaciones de grado inferior con coeficientes enteros. Este caso es fundamental en nuestra cuestión.

En el álgebra superior se demuestra que cualquier ecuación algebraica tiene por lo menos una raíz; por lo tanto, basándonos en el hecho de que cualquier polinomio se divide sin resto por $z - \alpha$ siendo α su raíz, podemos fácilmente expresar este polinomio como producto, o sea:

$$a_0z^n + a_1z^{n-1} + \cdots + a_n = a_0(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n), \tag{6.4}$$

donde α_1, ..., α_n son todas las n raíces del polinomio dado. Valiéndonos de la expresión del polinomio en forma de producto, podemos exponer la ecuación (6.2) de la siguiente forma:

$$a_0\left(\frac{x}{y}-\alpha_1\right)\left(\frac{x}{y}-\alpha_2\right)\cdots\left(\frac{x}{y}-\alpha_n\right) = \frac{c}{y^n} \tag{6.5}$$

Supongamos que existe una cantidad infinita de soluciones $[x_k, y_k]$ en números enteros para la ecuación (6.5). Esto significa que existen soluciones con un valor absoluto de y_k tan grande como se quiere. Si existiese una cantidad infinita de pares con y_k limitados y menores en valor absoluto que un número determinado cualquiera y con x_k tan grandes como se quiere, entonces, con estos x_k, el primer miembro de la ecuación (6.5) sería tan grande como se quiere mientras que el segundo miembro quedaría limitado, cosa imposible. Sea y_k muy grande. Entonces el segundo miembro de la ecuación (6.5) será pequeño y, por consiguiente, debe ser pequeño también el primer miembro. Mas el primer miembro de esta ecuación es el producto de n factores que contienen $\dfrac{x_k}{y_k}$ y a_0 el cual, siendo positivo, será no menor que 1. Por eso, la pequeñez del primer miembro de dicha ecuación puede condicionarse sólo por el hecho de que una de las diferencias

$$\frac{x_k}{y_k} - m$$

algebraicos mediante números algebraicos y teoría de los números transcendentes» (YMH4, N°4, 1949, pág. 19).

es pequeña por su valor absoluto. Está claro que esta diferencia puede ser pequeña únicamente cuando $\alpha?m$ es valor real, es decir, cuando no tiene lugar la igualdad $\alpha_m = \alpha + bi, b \neq 0$. De lo contrario el módulo de esta diferencia no puede ser tan pequeño como se quiera, puesto que

$$\left|\frac{x_k}{y_k} - a - bi\right| = \sqrt{\left(\frac{x_k}{y_k} - a\right)^2 + b^2} > |b|.$$

Dos diferencias y dos factores del primer miembro de la ecuación (6.5) no pueden ser, al mismo tiempo, pequeños por su módulo, puesto que

$$\left|\left(\frac{x_k}{y_k} - \alpha_m\right) - \left(\frac{x_k}{y_k} - \alpha_s\right)\right| = |\alpha_m - \alpha_s| \neq 0 \tag{6.6}$$

debido a que entre los valores am no hay dos que sean iguales. Si una de las diferencias, por su módulo o valor absoluto, es menor que $\frac{1}{2}|\alpha_m - \alpha_s|$ la otra, en virtud de la expresión (6.6), debe ser mayor que $\frac{1}{2}|\alpha_m - \alpha_s|$. Esto es debido a que el valor absoluto de la suma no supera la suma de los valores absolutos. Como todos los valores α_m son distintos entre sí, la diferencia más pequeña por su valor absoluto o módulo $|\alpha_m - \alpha_s|$, será mayor que cero $(m \neq s)$. Designando el valor de esta diferencia por $2d$, para algún valor de y_k lo suficiente grande (esto sucederá puesto que Yıt crece ilimitadamente) tendremos

$$\left|\frac{x_k}{y_k} - \alpha_m\right| < d$$

y, por consiguiente,

$$\left|\frac{x_k}{y_k} - \alpha_s\right| > d, \quad s = 1, 2, 3, ..., n \quad s \neq m \tag{6.7}$$

Entonces, puesto que el valor absoluto o módulo de un producto es igual al producto de los valores absolutos o módulos de sus factores, partiendo de la ecuación (6.5) tendremos

$$\left|a_0\left|\frac{x_k}{y_k} - \alpha_1\right| \cdots \left|\frac{x_k}{y_k} - \alpha_{m-1}\right|\left|\frac{x_k}{y_k} - \alpha_m\right| \left|\frac{x_k}{y_k} - \alpha_{m+1}\right| \cdots \left|\frac{x_k}{y_k} - \alpha_n\right|\right| = \frac{|c|}{|y_k|^n}. \tag{6.8}$$

Si en esta igualdad cambiamos cada una de las diferencias $\left|\frac{x_k}{y_k} - \alpha_s\right|$, $s \neq m$, por un valor menor d, y $|a_0|$ por la unidad, menor de la cual el número entero $|a_0|$ no puede ser, entonces el primer miembro de la expresión (6.8) se hace menor que el segundo, con lo que obtendremos la desigualdad

$$d^{m-1}\left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{|c|}{|y_k|^n},$$

o la desigualdad

$$\left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{c}{|y_k|^n}, \quad c_1 = \frac{|c|}{d^{n-1}}, \tag{6.9}$$

donde c_1 no depende de x_n ni de y_n. La cantidad de números α_m no es mayor que n y la cantidad de pares $[x_k, y_k]$, para los cuales con cualquier m se cumple la desigualdad (6.9), es multitud infinita. Por eso, existe un determinado m tal, que para un correspondiente α_m la desigualdad (6.9) se cumple una cantidad infinita de veces. Es decir, si la igualdad (6.1) tiene multitud infinita de soluciones en números enteros, entonces la ecuación algebraica (6.3), con coeficientes enteros, tiene una raíz α tal para la cual, siendo q un número tan grande como se quiera, se cumple la desigualdad

$$\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^n} \tag{6.10}$$

donde A es una constante que no depende de p ni de q; p y q, números enteros y n, el grado de la ecuación a la cual satisface α. Si fuese un número real arbitrario, entonces sería posible seleccionar este número de tal forma que para la desigualdad (6.10) realmente existiese una cantidad infinita de soluciones en números enteros p y q. Pero, en nuestro caso, a es raíz algebraica de una ecuación con coeficientes enteros. Tales números se llaman *algebraicos* y tienen propiedades especiales. Se llama *potencia de un número algebraico* al grado de aquella ecuación algebraica de grado mínimo con coeficientes enteros a la cual este número satisface.

A. Thue demostró que para un número algebraico α de n-ésimo grado la desigualdad

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{n}{2}+1}}, \quad n \geqslant 3, \tag{6.11}$$

puede tener solamente una cantidad finita de soluciones en números enteros p y q. Pero, siendo $n \geqslant 3$ y q lo suficiente grande, el segundo miembro de la desigualdad (6.10) se hace menor que el segundo miembro de la desigualdad (6.11) ya que $n > \frac{n}{2} + 1$. Por eso, si la desigualdad (6.11) puede tener solamente una cantidad

finita de soluciones en números enteros p y q, la desigualdad (6.10), con más razón, tiene solamente una cantidad finita de soluciones. Resulta, pues, que la ecuación (6.1) puede tener solamente una cantidad finita de soluciones enteras, cuando todas las raíces de la ecuación (6.3) no pueden ser raíces de una ecuación con coeficientes enteros de un grado inferior al n-ésimo. No es difícil comprobar que con $n = 2$ y un determinado A la desigualdad (6.10) puede tener, en efecto, una cantidad infinita de soluciones en números enteros p y q. Posteriormente el teorema de A. Thue fue reforzado considerablemente. Más, debemos señalar que el método utilizado para demostrar este teorema, en principio, no da posibilidad de hallar el límite superior para la magnitud de las soluciones, es decir, el límite de las posibles magnitudes de $|x|$ e $|y|$ con arreglo a sus coeficientes $a_0, a_1, \ldots, a_n$ y c. Este problema hasta hoy día no está resuelto. No dando posibilidad de determinar el limite de la magnitud de las soluciones, el procedimiento de A. Thue permite determinar el limite para la cantidad de soluciones de la ecuación (6.3) aunque bastante aproximado. Para distintas clases de ecuaciones deı tipo (6.3), este limite puede ser considerablemente definido. Por ejemplo, el matemático soviético B. N. Delone[2] demostró que la ecuación

$$ax^3 + y^3 = 1,$$

siendo a valor entero, puede tener además de solución trivial $x = 0, y = 1$, no más de una solución en números enteros x e y. También demostró que la ecuación

$$ax^3 + bx^2y + cxy^2 + dy^3 = 1$$

puede tener no más de cinco soluciones en números enteros x e y siendo enteros a, b, c y d.

Sea $P(x, y)$ un polinomio arbitrario con coeficientes enteros respecto a x e y, es decir,

$$P(x, y) = \sum A_{ks}x^k y^s,$$

donde A_{ks} son valores enteros. Acordaremos que este *polinomio es irreducible* cuando no se puede expresar en forma de producto de dos polinomios con coeficientes enteros, cada uno de los cuales no es simplemente un número.

K. Siegel, por un procedimiento especial y sumamente complicado, demostró que la ecuación

$$P(x, y) = 0,$$

donde $P(x, y)$ es un polinomio irreducible superior al segundo grado con respecto a x e y (es decir, cuando en él va incluido un término de la forma $A_{ks}x^k y^s$, siendo

[2]Este tema se trata en el ensayo de A. O, Guelfond «Teoría de los números», incluido en la recopilación «Las matemáticas en la URSS durante treinta años», Gostejizdat. M., 1948.

$k + s > 2$), puede tener una cantidad infinita de soluciones en números enteros x e y sólo si existen unos números

$$a_n, a_{n-1}, \ldots, a_0, a_{-1}, \ldots, a_{-n}$$

y

$$b_n, b_{n-1}, \ldots, b_0, b_{-1}, \ldots, b_{-n}$$

tales, que sustituyendo en nuestra ecuación x e y

$$x = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 + \frac{a_{-1}}{t} + \frac{a_{-n}}{t^n},$$
$$x = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_0 + \frac{b_{-1}}{t} + \frac{b_{-n}}{t^n},$$

obtenemos la identidad

$$P(x, y) \equiv 0$$

con relación a t. Aquí n es un número entero.

CAPÍTULO 7

Ecuaciones algebraicas de grado superior al segundo con tres incógnitas y algunas ecuaciones exponenciales

Si para ecuaciones con dos incógnitas podemos responder a la pregunta sobre la existencia de una cantidad finita o infinita de soluciones en números enteros, para ecuaciones con tres de dos incógnitas y de grado superior al segundo podemos dar respuesta a esta pregunta solamente para clases de ecuaciones sumamente particulares. No obstante, en este último caso se resuelve una cuestión más difícil como es la determinación de todas las soluciones de estas ecuaciones en números enteros. En calidad de ejemplo nos detendremos en el llamado gran teorema de Fermat.

El excelente matemático francés P. Fermat afirmaba que la ecuación

$$x^n + y^n = z^n, \tag{7.1}$$

siendo n valor entero y $n \geqslant 3$, no tiene soluciones en números enteros positivos x, y, z (el caso $xyz = 0$ se excluye por ser x, y, z positivos). No obstante a que P. Fermat afirmaba tener demostración (por lo visto, por el procedimiento de descenso, sobre el cual trataremos más adelante) esta demostración posteriormente no fue encontrada. Más aun, cuando el matemático Kummer intentó encontrar dicha demostración e incluso pensó un tiempo que la había encontrado, chocó con el hecho de que si una regla es justa para números enteros ordinarios, resulta injusta para formaciones numéricas más complejas, con las cuales, naturalmente, se tropieza en la investigación del problema de Fermat. Esto es debido a que los llamados *números algebraicos ente-*

ros, o sea, las raíces de ecuaciones algebraicas con coeficientes racionales enteros y con un coeficiente en la mayor potencia igual a 1, pueden ser descompuestos, por varios procedimientos, en factores enteros primos indescomponibles de la misma naturaleza algebraica. Por el contrario, los números ordinarios enteros se descomponen en factores primos por un solo procedimiento. Por ejemplo, $6 = 2 \cdot 3$ no tiene otra descomposición, dentro del conjunto de números ordinarios enteros, más que la dada. Si analizamos el conjunto de todos los números algebraicos enteros de la forma $m + n\sqrt{5}$, siendo m y n números ordinarios enteros, no será difícil observar que la suma y el producto de dos de estos números dan nuevamente números del mismo conjunto. El conjunto de números con la propiedad de contener cualesquiera sumas y productos de los mismos números que lo forman se llama *anillo*. Conforme a la definición dada, nuestro anillo contiene los números 2, 3, $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$. No es difícil comprobar que cada uno de los números de este anillo es primo, o sea, no puede ser expresado en forma de producto de dos números enteros, no iguales a la unidad, incluidos en nuestro anillo. Pero

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right),$$

es decir, en nuestro anillo, el número 6 se descompone en factores primos no solamente por un procedimiento. Lo mismo puede suceder en otros anillos más complejos de números algebraicos enteros. Al tropezar con esta circunstancia, Kummer se convenció de que su demostración del gran teorema general de Fermat no era cierta. Para superar las dificultades, relacionadas con la variedad de la descomposición en factores, Kummer construyó la teoría de ideales, la cual juega actualmente un papel sumamente importante en el álgebra y en la teoría de los números. Pero incluso mediante esta nueva teoría, Kummer no logró demostrar por completo el gran teorema de Fermat, y se limitó a demostrarlo solamente para n divisibles, al menos, por uno de los llamados números primos regulares. No deteniéndonos en el aclaramiento del contenido de número primo regular, indicaremos solamente que, hasta hoy en día, no se sabe si existe únicamente cantidad finita de estos números primos o multitud infinita de ellos.

Actualmente el gran teorema de Fermat está demostrado para muchos n, en particular, para cualquier n divisible por un número primo menor que 100. El gran teorema de Fermat jugó un papel importante en el desarrollo de las matemáticas debido a los intentos realizados con el fin de demostrar dicho teorema los cuales condujeron a la creación de la teoría de ideales. Debemos señalar que esta teoría fue creada con otros fines y por procedimientos completamente distintos por el excelente matemático ruso E. I. Zolotarev, fallecido en la cúspide de sus actividades científicas. La demostración del gran teorema de Fermat, sobre todo la demostración basada en los

razonamientos acerca de la teoría de la divisibilidad de los números, puede tener solamente interés particular. Claro, si esta demostración se logra por un procedimiento nuevo y fructífero, su importancia, junto con la importancia del propio procedimiento, puede ser muy grande. Mas los intentos realizados por aficionados a las matemáticas, también en nuestros tiempos, con el fin de demostrar el teorema de Fermat por procedimientos puramente elementales, están condenados al frkaso. Las consideraciones elementales, basadas en la teoría de la divisibilidad de los números fueron ya utilizadas por Kummer, y su posterior perfeccionamiento por parte de los más prominentes matemáticos, de momento, no han dado resultados notables.

A continuación daremos la demostración del teorema de Fermat para el caso de $n = 4$, ya que el *procedimiento de descenso*, a base del cual se construye la demostración, es muy interesante.

7.0.1 Teorema: La ecuación de Fermat

$$x^4 + y^4 = z^4 \tag{7.2}$$

no tiene soluciones en números enteros x, y, z; $xyz \neq 0$.

Demostración: Demostraremos un teorema incluso más general, precisamente, que la ecuación

$$x^4 + y^4 = z^2 \tag{7.3}$$

no tiene soluciones en números enteros x, y, z; $xyz \neq 0$. De este teorema ya se deduce directamente la ausencia de soluciones para la ecuación (7.2). Si la ecuación (7.3) tiene solución en números enteros distintos de cero x, y, z, entonces podemos suponer que estos números son dos a dos primos entre sí. En efecto, si existe una solución en la que x e y tienen máximo común divisor $d > 1$, entonces

$$x = dx_1 \quad \text{e} \quad y = dy_1$$

siendo $(x_1, y_1) = 1$. Dividiendo los dos miembros de la ecuación (7.3) por d^4 tendremos

$$x_1^4 + y_1^4 = \left(\frac{z}{d^2}\right)^2 = z_1^2. \tag{7.4}$$

Pero como x_1 e y_1 son números enteros, entonces $z_1 = \dfrac{z}{d^2}$ también es número entero. Si z_1 e y_1 tuviesen a $k > 1$ por divisor común, entonces, según la expresión (7.4), x sería divisible por k y, por lo tanto, x_1 y k no podrían ser primos entre sí. Resulta, pues, que existiendo solución de la ecuación (7.3) en números enteros diferentes a cero, existe también solución para esta ecuación en números enteros diferentes a cero y primos

entre sí. Por lo tanto basta con demostrar que la ecuación (7.3) no tiene soluciones en números enteros, diferentes a cero y primos entre sí dos a dos. Continuando la demostración y considerando que la ecuación (7.3) tiene solución, vamos a suponer que tiene solución en números enteros, positivos y primos entre sí dos a dos.

En el párrafo 3 hemos demostrado que todas las soluciones de la ecuación (3.1)

$$x^2 + y^2 = z^2 \tag{7.5}$$

en números enteros positivos y primos entre sí dos a dos, se hallan por la fórmula (3.7) y tienen la forma:

$$x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2}, \tag{7.6}$$

siendo u y v dos cualesquiera números impares positivos y primos entre sí.

Cambiemos un poco la forma de 'las fórmulas (7.6) mediante las cuales se determinan todas las soluciones de la ecuación (7.5). Puesto que u y v son números impares, suponiendo que

$$\frac{u+v}{2} = a \quad \text{y} \quad \frac{u-v}{2} = b, \tag{7.7}$$

podemos expresar u y v mediante las igualdades

$$u = a + b \quad \text{y} \quad v = a - b, \tag{7.8}$$

donde a y b son números enteros de distinta paridad. Las igualdades (7.7) y (7.8) demuestran que a cualquier par de números impares primos entre sí u y v, corresponde un par de números primos entre sí a y b de distinta paridad, y que a cualquier par de números primos entre sí a y b de distinta paridad, corresponde un par de números impares primos entre sí u y v. Por eso, sustituyendo en las fórmulas (7.6) u y v por a y b, tenemos que todos tres números x, y, z enteros positivos y primos entre sí dos a dos (x es impar) son soluciones de las ecuaciones (7.5) y se hallan por las fórmulas:

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2 \tag{7.9}$$

donde a y b son dos números cualesquiera primos entre sí de distinta paridad con la condición de que $x > 0$. Estas fórmulas demuestran que x e y son de distinta paridad. Si la ecuación (7.3) tiene solución $[x_0, y_0, z_0]$, esto significa que

$$[x_0^2]^2 + [y_0^2]^2 = z_0^2,$$

es decir, que los números (x_0^2, y_0^2, z_0) son solución de la ecuación (7.5). Pero entonces debe haber dos números a y b, $a > b$, primos entre sí y de distinta paridad, tales que

$$x_0^2 = a^2 - b^2, \quad y_0^2 = 2ab, \quad z_0 = a^2 + b^2. \tag{7.10}$$

Para precisar, admitimos que x_0 no es par y que y_0 es par. Admitiendo lo contrario no cambia nada, puesto que será suficiente cambiar x_0 por y_0 y viceversa. Pero sabemos ya (véase la igualdad (5.25)), que el cuadrado de un número impar, al ser dividido por 4, da de resto 1. Por eso de la igualdad

$$x_0^2 = a^2 - b^2 \tag{7.11}$$

se deduce que a es impar y b, par. De lo contrario, el primer miembro de esta igualdad, al ser dividido por 4, daría de resto 1 mientras que el segundo, puesto que hemos supuesto que a es par y b, impar, daría -1. Como a es impar y $(a, b) = 1$, entonces también $(a, 2b) = 1$. Pero, en este caso, de la igualdad

$$y_0^2 = 2ab$$

se deduce que

$$a = t^2, \quad 2b = s^2 \tag{7.12}$$

donde t y s son ciertos números enteros. Pero, de la relación (7.11) se desprende que $[x_0, b, a]$ es solución de la ecuación (7.5). Por lo tanto,

$$x_0 = m^2 - n^2, \quad b = 2mn, \quad a = m^2 + n^2,$$

donde m y n son ciertos números primos entre sí de diferente paridad. De la igualdad (7.12) tenemos que:

$$mn = \frac{b}{2} = \left(\frac{s}{2}\right)^2,$$

de aquí, puesto que m y n son primos entre sí, se deduce que

$$m = p^2, \quad n = q^2 \tag{7.13}$$

donde p y q son números enteros diferentes de cero. Como $a = t^2$ y $a = m^2 + n^2$, entonces

$$q^4 + p^4 = t^2. \tag{7.14}$$

Pero

$$z_0 = a^2 + b^2 > a^2.$$

Por lo tanto

$$0 < t = \sqrt{a} < \sqrt[4]{z_0} < z_0 \quad (z_0 > 1). \tag{7.15}$$

Considerando que $q = x_1, p = y_1$ y $t = z_1$, veremos que si existe la solución $[x_0, y_0, z_0]$, entonces también debe existir otra solución $[x_1, y_1, z_1]$, además, $0 < z_1 < z_0$. Este

proceso de obtención de soluciones de la ecuación (7.3) puede prolongarse ilimitadamente, con lo que obtendremos una sucesión de soluciones

$$[x_0, y_0, z_0], [x_1, y_1, z_1], \ldots, [x_n, y_n, z_n], \ldots,$$

además, los números enteros positivos $z_0, z_1, \ldots, z_n, \ldots$ disminuirán de un modo monótono, es decir, para ellos serán válidas las desigualdades

$$z_0 > z_1 > z_2 > \cdots > z_n \cdots$$

Pero los números enteros positivos no pueden formar una sucesión infinita que decrece monótonamente, ya que dicha sucesión no puede tener más que z_0 términos. Así, pues, hemos llegado a una contradicción al suponer que la ecuación (7.3) tiene, por lo menos, una solución en números enteros x, y, z; $xyz \neq 0$. Con ello se demuestra que la ecuación (7.3) no tiene soluciones. Por lo tanto, la ecuación (7.2) tampoco tiene soluciones en números enteros positivos $[x, y, z]$, ya que de lo contrario, o sea, siendo $[x, y, z]$ solución de la ecuación (7.2), $[x, y, z^2]$ será solución de la ecuación (7.3).

El método de demostración que acabamos de utilizar y que consiste en desarrollar, mediante una solución, una sucesión infinita de soluciones en las que z es valor positivo ilimitadamente decreciente se llama método de descenso. Como ya indicábamos anteriormente, emplear este método para el caso general del teorema de Fermat, por ahora, lo impide la falta de unicidad en la descomposición de los números enteros de anillos algebraicos en factores primos pertenecientes a estos mismos anillos[1]. □

Observaremos que hemos demostrado la ausencia de soluciones enteras no sólo para la ecuación. (7.3), sino también para la ecuación

$$x^{4n} + y^{4n} = z^{2n}$$

Es curioso también que la ecuación

$$x^4 + y^4 = z^2,$$

tiene multitud infinita de soluciones en números enteros positivos, por ejemplo, $x = 2, y = 3, z = 5$. Proponemos a nuestros lectores hallar la forma de todas las soluciones de esta ecuación, en números enteros positivos x, y, z.

Veamos otro ejemplo de la aplicación del método de descenso, cambiando un poco el orden de los razonamientos.

[1]Para un mejor conocimiento del gran teorema de Fermat, recomendamos al lector el libro de A. Ya. Jinchin «El gran teorema de Fermat», ITTH, M., 1934.

7.0.2 Ejemplo Demostremos que la ecuación

$$x^4 + 2y^4 = z^2 \tag{7.16}$$

no tiene solución en números enteros diferentes de cero x, y, z. Supongamos que la ecuación (7.16) tiene solución en números enteros positivos $[x_0, l'o.\ z_0)$. Inmediatamente podemos considerar que estos húmeros son primos entre sí, puesto que si tuviesen máximo común divisor $d > 1$, entonces los números $\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}$ también serian solución de la ecuación (7.16). La existencia de un divisor común para dos de ellos presupone la existencia de divisor común para los tres. Supongamos, además, que z_0 es mínimo entre todos los posibles z en las soluciones de la ecuación (7.16) en números enteros positivos. Como quiera que $[x_0, y_0, z_0]$ es solución de la ecuación (7.16), entonces $[x_0^2, y_0^2, z_0^2]$ será solución de la ecuación

$$x^2 + 2y^2 = z^2 \tag{7.17}$$

Valiéndonos de las fórmulas (3.9) párrafo 3, las cuales dan todas las soluciones enteras positivas de la ecuación (7.17), veremos que existen unos valores enteros positivos a y b, $(a,\ b) = 1$, siendo a impar, tales que verifican las igualdades

$$x_0^2 = \pm(a^2 - 2b^2), \quad y_0^2 = 2ab, \quad z_0 = a^2 + 2b^2. \tag{7.18}$$

De la igualdad $y_0^2 = 2ab$ se deduce que b debe ser par, puesto que y_0 es par; y_0^2 divisible por 4 y a impar. Como $\frac{b}{2}$ y a son

$$\left(\frac{y_0}{2}\right)^2 = a\frac{b}{2}$$

se deduce directamente que

$$a = m^2, \quad \frac{b}{2} = n^2,$$

donde m y n son números enteros positivos y $(m,\ 2n) = 1$. Pero de las igualdades (7.18) se desprende que:

$$x_0^2 = \pm(a^2 - 2b^2) = \pm\left[a^2 - 8\left(\frac{b}{2}\right)^2\right], \tag{7.19}$$

donde x_0 y a son impares. Anteriormente hemos visto que el cuadrado de un número impar al ser dividido por 4 da 1 de resto. Por consiguiente, el primer miembro de la expresión (7.19) al ser dividido por 4 dará 1 de resto; también dará 1 de resto, al ser dividida por cuatro, la expresión $a^2 - 8\left(\frac{b}{2}\right)^2$. Resulta, pues, que el paréntesis en el segundo miembro de la ecuación (7.19) puede tener solamente signo positivo. Ahora, la ecuación (7.19) puede ya expresarse de la forma:

$$x_0^2 = m^4 - 8n^4$$

o de la forma

$$x_0^2 + 2(2n^2)^2 = (m^2)^2, \tag{7.20}$$

donde x_0, n y m son números positivos primos entre sí. Por lo tanto, x_0, $2n^2$, m^2 son la solución de la ecuación (7.17), además, x_0, $2n^2$ y m^2 son primos entre sí. Por eso, basándonos en las fórmulas (3.8) del párrafo 3, podemos hallar unos números enteros p y q (p, impar y $(p, q) = 1$), tales que

$$2n^2 = 2pq, \quad m^2 = p^2 + 2q^2, \quad x_0 = \pm(p^2 - 2q^2). \tag{7.21}$$

Pero como $(p, q) = 1$ y $n^2 = pq$, entonces

$$p = s^2, \quad q = r^2,$$

donde s y r son números enteros primos entre sí. De aquí se deduce finalmente la relación

$$s^4 + 2r^4 = m^2, \tag{7.22}$$

la cual demuestra que los números s, r, y m son la solución de la ecuación (7.16). Pero de las igualdades obtenidas anteriormente

$$z_0 = a^2 + 2b^2, \quad a = m^2,$$

se deduce que $z_0 > m$. O sea, teniendo la solución $[x_0, y_0, z_0]$ hallamos otra solución $[s, r, m]$, además $0 < m < z_0$. Esto, naturalmente, contradice la suposición, hecha por nosotros, de que la solución $[x_0, y_0, z_0]$ tiene un z_0 mínimo entre todos los posibles. Así, pues, admitiendo la existencia de soluciones para la ecuación (7.16) hemos llegado a una contradicción y, al mismo tiempo, hemos demostrado que esta ecuación no tiene solución en números enteros diferentes de cero.

Ahora proponemos a nuestros lectores demostrar que las ecuaciones:

$$x^4 + 4y^4 = z^2, \quad x^4 - y^4 = z^2,$$
$$x^4 - y^4 = 2z^2, \quad x^4 - 4y^4 = z^2$$

no tienen solución en números enteros positivos.

Finalmente, haremos algunas objeciones sobre las ecuaciones exponenciales. *La ecuación*

$$a^x + b^y = c^z. \tag{7.23}$$

donde a, b y c son números enteros no iguales a la potencia de dos y al cero, puede tener no más que una cantidad finita de soluciones en números enteros x, y, z. Esta misma afirmación, con una condición suplementaria no muy esencial, es también válida cuando a, b y c son números algebraicos arbitrarios. Más aún, la ecuación:

$$A\alpha_1^{x_1}...\alpha_n^{x_n} + B\beta_1^{y_1}...\beta_m^{y_m} + C\gamma_1^{z_1}...\gamma_p^{z_p} = 0 \tag{7.24}$$

donde A, B, C ($ABC \neq 0$) son valores enteros, α_1, ..., α_n, β_1, ..., β_m, γ_1, ..., γ_p números enteros y α, β, γ,

$$\alpha = \alpha_1...\alpha_n \quad \beta = \beta_1...\beta_n, \quad \gamma = \gamma_1...\gamma_n,$$

números primos entre sí, puede tener solamente una cantidad finita de soluciones en números enteros $x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_p$. Esta afirmación también es válida si A, B, C y $\alpha?\iota, \beta_k, \gamma_s$ son valores algebraicos[2]. Las ecuaciones del tipo (7.24) y sus generalizaciones representan gran interés puesto que en ta teoría de los números algebraicos se demuestra que a cada ecuación algebraica del tipo (6.1) corresponde cierta ecuación exponencial del tipo (7.24) además, a cada solución de la ecuación (6.1) corresponde una solución de la ecuación (7.24) en números enteros. Esta correspondencia se extiende también a las ecuaciones de tipo más general que las del tipo (6.1) y (7.24).

[2]Véase el ensayo de A. O. Guelfond, al cual nos referimos en la pág. 53.

A nuestros lectores

«Mir» edita libros soviéticos traducidos al español, inglés, francés, árabe y otros idiomas extranjeros. Entre ellos figuran las mejores obras de las distintas ramas de la ciencia y la técnica: manuales para los centros de enseñanza superior y escuelas tecnológicas, literatura sobre ciencias naturales y medicas. También se incluyen monografías, libros de divulgación científica y ciencia-ficción.

Dirijan sus opiniones a la Editorial «Mir», 1 Rizhski per., 2, 129820, Moscú, I-110, GSP, URSS.